(Grund-)Recht auf Verschlüsselung?

Vom Fachbereich Rechts- und Wirtschaftswissenschaften der
Technischen Universität Darmstadt genehmigte

Dissertation

zur Erlangung des akademischen Grades eines Doctor iuris (Dr. iur.)
Vorgelegt von

Ass. iur. Julia Gerhards
Magister en Derecho Internacional y Relaciones Internacionales,
Universidad Complutense de Madrid

Geburtsdatum: 10.09.1976
Geburtsort: Köln

Erstgutachterin: Prof. Dr. Viola Schmid, LL.M. (Harvard)
Zweitgutachter: Prof. Dr. Jochen Marly

Eingereicht am: 17.12.2009
Mündliche Prüfung am: 11.02.2010
Darmstadt 2010
D 17

Dieses Dokument entspricht ab der folgenden Seite – auch hinsichtlich der insoweit zitierbaren Seitenzahlen – der Buchveröffentlichung:

Julia Gerhards, (Grund-)Recht auf Verschlüsselung?,
Reihe „Der elektronische Rechtsverkehr“, hrsg. von Prof. Dr. Alexander Roßnagel in Zusammenarbeit mitdem TeleTrusT Deutschland e.V., Band 23, Nomos Verlagsgesellschaft, Baden-Baden 2010, ISBN 978-3-8329-5704-9

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2009/2010 von der Technischen Universität Darmstadt als Dissertation angenommen. Für die vorliegende Veröffentlichung konnte der Stand von Literatur und Gesetzgebung bis März 2010 berücksichtigt werden.

An allererster Stelle möchte ich Frau Prof. Dr. Viola Schmid, LL.M. (Harvard) für die intensive Betreuung der Arbeit und die gewährten – inneren wie äußeren – Freiräume danken. Dadurch hatte ich die Ressourcen und die gedankliche Freiheit, meinem eigenen Weg nachzugehen. Dabei stand ihre Tür stets offen. Herzlichen Dank für die inspirierenden Diskussionen und die weiterführende Kritik, die immer exakt den Punkt traf.

Besonderer Dank gilt daneben Herrn Prof. Dr. Jochen Marly für die zügige Erstellung des Zweitgutachtens und die bereichernden Anmerkungen.

Herrn Prof. Dr. Alexander Roßnagel danke ich sehr für die Aufnahme der Arbeit in die Schriftenreihe „Der elektronische Rechtsverkehr".

Die Arbeit entstand in Folge des vom Bundesministerium für Bildung und Forschung geförderten Projekts SicAri („Eine Sicherheitsplattform und deren Werkzeuge für die ubiquitäre Internetnutzung"). Die Verfasserin dankt den beteiligten Projektpartnern und dem Ministerium für die Förderung.

Ganz besonders möchte ich mich schließlich für die Gewährung eines Druckkostenzuschusses aus Frauenfördermitteln des Fachbereichs Rechts- und Wirtschaftswissenschaften bedanken.

Viele Kollegen, Freunde und Verwandte haben mich in der Zeit der Promotion begleitet und unterstützt. Ihnen allen möchte ich danken. Einigen gebührt aber ganz besondere Erwähnung: Patrick G. Stößer, ohne den ich niemals über Verschlüsselung nachgedacht hätte, Andrea Junglas, Heike Krückel-Diehl, Laima Nader und Julia Pieh, die mir immer mit Rat und Tat zur Seite standen, und allen voran meiner Familie, die Freud und Leid der Promotion mit mir geteilt und mich stets ermutigt hat.

Darmstadt im Mai 2010 *Julia Gerhards*

Inhaltsverzeichnis

Abkürzungsverzeichnis

ABl.	Amtsblatt
AöR	Archiv des öffentlichen Rechts
Anm.	Anmerkung
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKAG	Gesetz über das Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
CIC	Codex Iuris Canonici
CPU	Central Processing Unit
CR	Computer und Recht
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DÖV	Die Öffentliche Verwaltung
DRiZ	Deutsche Richterzeitung
DSB	Datenschutzberater
DuD	Datenschutz und Datensicherheit
DVBl	Deutsches Verwaltungsblatt
EGMR	Europäischer Gerichtshof für Menschenrechte
EuG	Europäisches Gericht erster Instanz
EuGH	Europäischer Gerichtshof
FN	Fußnote
GA	Generalanwalt
GV. NRW	Gesetzes- und Verordnungsblatt des Landes Nordrhein-Westfalen
HGR	Handbuch der Grundrechte
HStR	Handbuch des Staatsrechts
IEC	International Electrotechnical Commission
InfSpekt	Informatik Spektrum
IPbpR	Internationaler Pakt über bürgerliche und politische Rechte
ISO	International Organization for Standardization
JZ	Juristenzeitung
KritJ	Kritische Justiz
KritV	Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft
K&R	Kommunikation und Recht
LAN	Local Area Network
MAC	Message Authentication Code

MDR	Monatsschrift für Deutsches Recht
MMR	Multimedia und Recht
NJW	Neue Juristische Wochenschrift
NJW-CoR	Computerreport der Neuen Juristischen Wochenschrift
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
PDA	Personal Digital Assistant
PR ITR	PraxisReport IT-Recht (juris)
RdV	Recht der Datenverarbeitung
RFC	Request for Comments
RFID	Radio Frequency Identification
StAnz	Staatsanzeiger
StraFo	Strafverteidiger-Forum
TKÜ	Telekommunikationsüberwachung
TKÜV	Telekommunikations-Überwachungsverordnung
U. Pa. L. Rev.	University of Pennsylvania Law Review
VBlBW	Verwaltungsblätter Baden-Württemberg
WiGBL.	Gesetzblatt der Verwaltung des Vereinigten Wirtschaftsgebietes
WLAN	Wireless Local Area Network

Glossar

Algorithmus	genau definierte Handlungsvorschrift zur Lösung eines Problems oder einer bestimmten Art von Problemen in endlich vielen Schritten
Asymmetrische Verschlüsselung	Verschlüsselungsverfahren, bei denen für die Ver- und Entschlüsselung verschiedene Schlüssel eines Schlüsselpaars, bestehend aus jeweils einem öffentlichen und einem privaten Schlüssel, verwendet werden
Body	Inhalt eines Datenpakets, im Gegensatz zum sog. Header, dem Kopfbereich eines Datenpakets
Brute-Force-Angriff	eine Angriffsmethode, die im Ausprobieren aller denkbaren Möglichkeiten besteht
Chiffretext	In der Kryptographie werden verschlüsselte Daten (in Abgrenzung zu unverschlüsselten Daten) als Chiffretext bezeichnet (oder auch `cyphertext´)
Ciphertext	s. Chiffretext
Client	auch als Dienst bezeichnet; ein Computerprogramm, das Kontakt zu einem Server aufnimmt, um dessen Dienstleistung zu nutzen
Cookie	Dateien auf dem Rechner des Nutzers, die nutzerbezogene Informationen speichern
DES	`Data Encryption Standard´, ein symmetrischer Verschlüsselungsalgorithmus
Distributed Denial of Service-Attacke	Angriff auf ein informationstechnisches System, bei dem von einer Vielzahl von Rechnern Anfragen gestellt werden, um das angegriffene System durch Überlastung funktionsuntüchtig zu machen
Dual-Use-Technologie	Technologie mit doppeltem Verwendungszweck, d.h. in der Regel für zivile als auch militärische Zwecke
Einmalverschlüsselung	engl. `One-Time-Pad´. Ein mathematisch beweisbar absolut sicheres Verschlüsselungsverfahren, bei dem die zu verschlüsselnden Daten Zeichen für Zeichen (oder Bit für Bit) mit einem mindestens ebenso langen Zeichen- oder Datensatz verknüpft werden
Einwegfunktion	engl. `one-way function´. Funktionen, die effizient berechnet werden können, für deren Umkehrfunktion aber kein effizientes Berechnungsverfahren bekannt ist
Einwegfunktion mit Falltür	engl. `trap door one-way function´. Einwegfunktion, deren Umkehrfunktion mit Hilfe einer Zusatzinformation (der Falltür) effizient berechnet werden kann
E-Mail-Server	Soft- oder Hardware, die E-Mails verwaltet (empfängt, sendet, speichert)
Ende-zu-Ende-Verschlüsselung	Verschlüsselung, bei der die Daten beim Sender ver- und erst beim Empfänger wieder entschlüsselt werden; im

	Gegensatz zur abschnittsweise erfolgenden Leitungsverschlüsselung
Hashfunktion	Funktion zur Bildung des Hashwerts
Hashwert	Prüfsumme eines Datensatzes, auch als Fingerabdruck bezeichnet
Header	Kopfbereich eines Datenpakets, der Informationen zum Transport des Pakets enthält
IDEA	`International Data Encryption Algorithm´, ein symmetrischer Verschlüssselungsalgorithmus
Intranet	nicht-öffentliches, internes Rechnernetz
IP-Adresse	Adresse in Computernetzen, die auf dem `Internet Protocol´(IP) basieren, wie z.B. das Internet
Key escrow	Verschlüsselungsverfahren, bei denen die Schlüssel verpflichtend zu hinterlegen sind
Key recovery	Verschlüsselungsverfahren mit einer technisch implementierten Möglichkeit, einen Nachschlüssel zu erzeugen
Keylogger	Hard- oder Software, die Tastatureingaben protokolliert
Klartext	engl. `plaintext´. In der Kryptographie werden die Daten vor ihrer Verschlüsselung häufig Klartext genannt
Kryptoanalyse	Lehre der Gewinnung von Information aus verschlüsselten Texten / Daten
Kryptographie	„Lehre vom verborgenen Schreiben“; Verschlüsselung
Kryptologie	Oberbegriff für Kryptographie und Kryptoanalyse
LAN	Local Area Network
Leitungsverschlüsselung	Verschlüsselung, bei der alle Daten zwischen zwei physikalischen Endpunkten verschlüsselt werden
Less-Than-Zero-Day Exploit	Angriffsprogramm, das bisher unbekannte oder unveröffentlichte Sicherheitslücken ausnutzt
Log-Datei	Datei mit dem automatisch geführten Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem
Message Authentication Code	Hashfunktion, die zusätzlich noch einen geheimen Schlüssel verwendet
Öffentlicher Schlüssel	engl. `public key´; der zu veröffentlichende Teil eines Schlüsselpaares in asymmetrischen Verschlüsselungsverfahren
One-Time-Pad	s. Einmalverschlüsselung
One-way function	s. Einwegfunktion
Plaintext	s. Klartext
Private key	s. privater Schlüssel
Privater Schlüssel	engl. `private key´; der geheim zu haltende Teil eines Schlüsselpaares in asymmetrischen Verschlüsselungsverfahren
Proxy	Vermittlungsrechner, die ausgehende Datenpakete unter ihrer eigenen IP-Adresse weiterleitenen und eingehende Datenpakete an den Empfänger weiterreichen

Public key	s. öffentlicher Schlüssel
Public Key Infrastruktur	Infrastruktur zur Verwaltung öffentliche Schlüssel
Public Key Kryptographie	Synonym für asymmetrische Verschlüsselungsverfahren
Quantencomputer	Computer, dessen Funktion auf den besonderen Gesetzen der Quantenmechanik beruht, und der, sollte seine Realisierung gelingen, exorbitant leistungsfähiger als heutige Computer wäre
Quellen-TKÜ	Quellen-Telekommunikationsüberwachung; Verfahren zur Überwachung von Internettelefonie im Wege der Infiltration der Endgeräte
RFC	Request for Comments; zunächst informelle technische und organisatorische Dokumente insbes. zur Funktionsweise des Internets, die später teilweise de facto zum Standard werden
Router	Vermittlungsrechner, die Datenpakete weiterleiten
Seitenkanalangriff	Angriff auf die physikalische Implementierung von Verschlüsselungsverfahren, der versucht, aus äußerlich physikalisch messbaren Größen wie Rechenzeit, Stromverbrauch oder elektromagnetischer Abstrahlung Rück - schlüsse auf ausgeführte Rechenoperationen zu erlangen
Smartcard	Chipkarten, die eine Hardware-Logik, Speicher oder auch einen Mikroprozessor enthalten
Social engineering	Angriffe auf nicht-technischem Wege durch zwischenmenschliche Beeinflussung
stand-alone-System	physisch gänzlich von anderen informationstechnischen Systemen, Intranets und dem Internet losgelöstes System
Steganographie	„Lehre vom verdeckten Schreiben“, die geheime Nachrichtenübermittlung durch ein Verstecken der Nachricht erreichen will
Symmetrische Verschlüsselung	Verschlüsselungsverfahren, bei denen zur Ver- und Entschlüsselung der gleiche Schlüssel verwendet wird
Token	Hardwarekomponente, die Teil eines Systems zur Identifizierung und Authentifizierung von Benutzern ist
Triple-DES	ein symmetrischer Verschlüsselungsalgorithmus
Web of trust	„Netz des Vertrauens“, in dem Nutzer untereinander die die Echtheit von öffentlichen Schlüsseln durch digitale Signaturen bestätigen
Webserver	Computer, auf denen Webseiten und andere Internetinhalte gespeichert sind, und der diese Inhalte z.B. an Web browser überträgt
WLAN	Wireless Local Area Network
Wörterbuchangriff	Angriff auf Passwörter durch Ausprobieren von Passwörtern anhand einer Passwortliste
Zero-Day Exploit	Angriffsprogramm, das bekannte Sicherheitslücken ausnutzt, in der Regel kurz nach deren Bekanntwerden, so dass entweder noch kein Patch vorhanden oder noch nicht von allen Nutzern installiert ist

Gerichtsentscheidungen werden – soweit nicht anders angegeben – nach den jeweiligen online verfügbaren Entscheidungssammlungen zitiert, verfügbar unter:

Bundesverfassungsgericht	http://www.bverfg.de/[1]
Bundesverwaltungsgericht	http://www.bundesverwaltungsgericht.de/
Bundesgerichtshof	http://www.bundesgerichtshof.de/
Europäischer Gerichtshof	http://curia.europa.eu/jcms/jcms/Jo1_6308/
Europäischer Gerichtshof für Menschenrechte	http://www.echr.coe.int/

Wikipedia wird unter Nennung der verwendeten Version und des Permanentlinks zitiert.[2]

Sonstige Internetquellen werden soweit möglich unter Angabe des Permanentlink zitiert, im Übrigen unter Nennung von Internetadresse und letztem Abrufdatum.

Soweit ein Zeilenumbruch innerhalb der Internetadresse erforderlich ist, wir lediglich ein Leerzeichen eingefügt. Auf Trennstriche wird verzichtet, um keine Verwechslungsgefahr mit eventuell zur Internetadresse gehörenden Bindestrichen zu schaffen.

1 Alle Entscheidungen ab 01.01.1998.

2 Vgl. zu Zitierfähigkeit und Zitierweise von Wikipedia *Zosel*, Im Namen des Volkes: Gerichte zitieren Wikipedia, JurPC 140/2009, verfügbar unter: http://www.jurpc.de/aufsatz/20090140.htm (08.12.2009).

Einleitung

Die Digitalisierung hat unseren Lebensalltag in nahezu allen Bereichen signifikant verändert. Ob die Bezeichnung „Informationsgesellschaft“ das richtige Etikett dafür darstellt, kann diskutiert werden; Fakt ist, dass Information oder Wissen[3] zentrales (Wirtschafts-)Gut unserer Gesellschaft ist. Wer über welche Informationen verfügt oder nicht verfügt, ist essentielle Frage bei der Verteilung von Risiken und Chancen. Herrschaft über Information begründet unmittelbar Macht. Die Frage, „wer was wann und bei welcher Gelegenheit“[4] weiß, ist nicht Obsession technikfeindlicher *`Digital Immigrants´*[5] oder sogar *`Digital Exiles´*[6], sondern zentrale Verteilungsentscheidung.

Verschlüsselung ist ein hocheffektives Instrument zur Beherrschung (digitaler) Information. Es ist insoweit wenig verwunderlich, dass Verschlüsselung lange Zeit Geheimwissen und Privileg einiger Weniger war. Heute sind Verschlüsselungstechnologien Massenware. Die Beantwortung der Frage, wem dieses Instrument zu welchen Zwecken zur Verfügung stehen soll und welche staatlichen Informationsbedürfnisse mit welcher Zielsetzung (von der Steuerschätzung über Infrastrukturplanung bis zur Verbrechensprävention) notwendig und legitim sind, beinhaltet fundamentale Entscheidungen, die die Zukunft unserer Gesellschaft maßgeblich gestalten werden.

Eine solch komplexe Frage kann natürlich aus verschiedenen Blickwinkeln beleuchtet, diskutiert und beantwortet werden. Hier wird eine (grund-)rechtliche Analyse versucht.

Dabei wird in einem Teil 1 überblicksartig die Funktionsweise von Verschlüsselungsverfahren erläutert. Diese technische Einführung in Verschlüsselung soll dem Leser ein *grundlegendes* Verständnis von Verschlüsselung ermöglichen. Auf alle detaillierteren Informationen wurde verzichtet, um nur die für das Verständnis dieser Arbeit wesentlichen Aspekte in der notwendigen Kürze und Klarheit herauszuarbeiten. Dabei enthält sich die Darstellung der technischen Funktionsweise von Verschlüsselung und ihrer Bedeutung in einer technischen Perspektive (Teil 1 unter A. und B.) *jeglicher* rechtlicher (Be-)Wertung. Erst in der anschließenden Darstellung

3 So dass zum Teil eher von einer Wissensgesellschaft gesprochen wird.

4 BVerfGE 65, 1, 43 – Volkszählungsurteil.

5 Als *`Digital Immigrants´* werden Personen bezeichnet, die erst im Erwachsenenalter mit digitalen Technologien in Berührung gekommen sind – als Gegenbegriff zu den sog. *`Digital Natives´*, also Personen, die mit digitalen Technologien aufgewachsen sind; vgl. Wikipedia, Digital Native, Version vom 19.11.2009, 18.16 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Digital_Native&oldid=67016423.

6 In Anlehnung an die eben vorgestellte Terminologie könnte man Personen, die die Nutzung digitaler Technologien verweigern, als „ Im digitalen Exil Lebende“ bezeichnen.

der Bedeutung von Verschlüsselung in einer einfachgesetzlichen Perspektive (Teil 1 unter C.) werden rechtliche Aspekte und Wertungen eingeführt.

Sodann werden in Teil 2 paradigmatische Szenarien des Umgangs mit Verschlüsselung entwickelt, die dann in den Teilen 3 bis 6 jeweils verfassungsrechtlich untersucht werden. Teil 7 beschließt die Arbeit mit einer Zusammenfassung der erarbeiteten Ergebnisse und einem Ausblick in die Zukunft.

Schon immer hatten Menschen das Bedürfnis, geheime Nachrichten auszutauschen - aus privaten, militärischen, diplomatischen Motiven. Verschlüsselungsverfahren dienen seit jeher der Gewährleistung der Vertraulichkeit von Kommunikation. Die „Lehre vom verborgenen Schreiben", die Kryptographie (von griech.: *‚kryptós'* „verborgen" bzw. *‚kryptein'* „verbergen" und *‚gráphein'* „schreiben"[7]), ist bereits mehr als 3.000 Jahre alt.[8]

Frühe, klassische Verschlüsselungsverfahren (A.I.) ersetzten dabei zunächst jeweils ein bestimmtes Zeichen durch ein bestimmtes anderes Zeichen. Ausgefeiltere Techniken vertauschten zudem einzelne Zeichen oder Zeichenblöcke. Natürliche Grenze blieb dabei aber immer das, was bei Ver- und Entschlüsselung per Hand (noch) durchführbar war. Die Computertechnologie hat insoweit zu einem Quantensprung in der Kryptographie geführt:

- Zum einen hinsichtlich der Komplexität von Verschlüsselungsverfahren: Die der Ver- und Entschlüsselung immanente Grenze des menschlich Machbaren an Rechenoperationen wurde aufgehoben, da mit der Computertechnologie die (zeit- und ressourcenadäquat) „machbaren" Rechenoperationen exponentiell anstiegen. Die zunehmende Komplexität von Verschlüsselungsverfahren wurde auch notwendig, da derselbe Kapazitätszuwachs an (zeit- und ressourcenadäquat) realisierbaren Rechenoperationen zugleich auch der Kryptoanalyse zukam, die sich - sozusagen als Gegenstück zur Kryptographie - mit der Gewinnung von Informationen aus verschlüsselten Texten befasst.
- Zum anderen hinsichtlich der Verbreitung von Verschlüsselungsverfahren: Mit der zunehmenden Verbreitung der Computertechnologie stand das Instrumentarium für hochkomplexe Verschlüsselungsverfahren plötzlich einem breiten Personenkreis zur Verfügung, nachdem Verschlüsselung jahrtausendelang im Wesentlichen ein Privileg von Militär, Diplomatie und Herrschaftseliten gewesen ist. Neben der Notwendigkeit komplexerer Verschlüsselungsverfahren waren es vor allem die Herausforderungen dieser (möglichen) Breitennutzung von Verschlüsselung, die zur Entwicklung moderner Verschlüsselungsverfahren (A.II.) führten.

7 *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 14.

8 So wurden etwa laut *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 11 bereits 1500 vor Christus Geheimzeichen verwendet, um Informationen, in dem Fall das Rezept für eine Tonglasur, zu bewahren und zu schützen.

I. Klassische Verschlüsselungsverfahren

Klassische Verschlüsselungsverfahren wandeln einen Ausgangstext (den Klartext, häufig auch als `*plaintext´* bezeichnet[9]) durch Kombination mit einem bestimmten Zeichensatz, dem Schlüssel, in eine andere Zeichenkombination (den Chiffretext oder `*cyphertext´*) um. Ziel ist, dass aus dem Chiffretext ohne Kenntnis des Schlüssels nicht der Klartext ermittelt werden kann.

1. Substitution

Eine Grundmethode klassischer Verschlüsselungsverfahren ist die Substitution.[10] Substitution bedeutet das Ersetzen einzelner Zeichen oder Zeichenblöcke durch andere Zeichen. Ein einfaches Beispiel ist die Caesar-Verschlüsselung. Dabei wird das Alphabet durch Verschiebung um eine festzulegende Anzahl von Buchstaben auf ein anderes Alphabet abgebildet. So wird etwa aus

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

bei der Verschiebung um vier Stellen folgendes Alphabet

E F G H I J K L M N O P Q R S T U V W X Y Z A B C D.

Als Schlüssel würde man hier "E" bezeichnen, weil ein „A" auf ein „E" abgebildet wird. Bei Verschlüsselung des Satzes

DIESE VERSCHLUESSELUNGSMETHODE IST SICHER.

durch Ersetzung der einzelnen Buchstaben würde der Chiffretext wie folgt aussehen:

HMIWI ZIVWGLPYIWWIPYRKWQIXLSHI MWX WMGLIV.

Die Zeichen können zudem als Fließtext dargestellt werden, so dass nicht erkennbar ist, wie lang die einzelnen Worte sind.

HMIWIZIVWGLPYIWWIPYRKWQIXLSHIMWXWMGLIV.

Oder die Zeichenfolge wird in gleichmäßige Blöcke aufgeteilt.

HMIW IZIV WGLP YIWW IPYR KWQI XLSH IMWX WMGL IV.

9 Bundesamt für Sicherheit in der Informationstechnik, E-Government-Handbuch: Verschlüsselung und Signatur, verfügbar unter: http://www.bsi.de/fachthem/egov/download/2_Krypto.pdf (26.02.2008), S. 16.

10 Siehe verschiedene Substitutionsverfahren bei *Pohlmann/Hesse,* ITSD 2006, 430, 431 ff.

Das Verfahren ist natürlich äußerst simpel und der Chiffretext könnte von einem interessierten Dritten ohne größere Mühe entziffert werden: Eine der grundlegenden Techniken der Kryptoanalyse ist die Analyse von Buchstabenhäufungen. So kommen im Deutschen etwa ein E oder ein A bedeutend häufiger vor als ein X oder ein Y.[11] Bei einer reinen Verschiebung des Alphabets bleiben diese Häufigkeiten vollständig erhalten, so dass nach Ermittlung der Buchstabenhäufigkeiten nur noch wenige Varianten übrig bleiben, die dann durch schlichtes Ausprobieren getestet werden können.

2. Permutation

Neben der Substitution ist eine weitere grundlegende Methode die Permutation.[12] Dabei werden einzelne Zeichen oder Zeichenblöcke nach einem bestimmten Schema in ihrer Reihenfolge vertauscht.[13] Mehrere Substitutionen und Permutationen können natürlich auch hintereinander durchgeführt werden, was eine Entschlüsselung ohne Kenntnis der verwendeten Verfahren weiter erschwert.

Mit der modernen Computertechnologie stehen heute allerdings völlig andere Möglichkeiten offen, solche mit klassischen Methoden verschlüsselten Texte zu analysieren und somit zu entschlüsseln. Buchstabenhäufigkeiten können heute viel schneller und effektiver analysiert werden, mögliche Verschlüsselungsverfahren können schlicht ausprobiert werden.

3. Einmalschlüssel-Verfahren

Ein weiteres klassisches Verschlüsselungsverfahren ist das Einmalschlüssel-Verfahren.[14] Es kann insoweit als eigenständige Kategorie von Verfahren betrachtet werden als es weder auf Permutationen noch auf Substitutionen basiert. Dabei ist es zugleich das einzige Verschlüsselungsverfahren, das mathematisch beweisbar *absolut* sicher ist: *Ohne Kenntnis des Schlüssels ist es praktisch und theoretisch unmöglich, den verschlüsselten Text zu entschlüsseln*. Das *`One-Time-Pad´* (Einmalverschlüsselung oder Einmalschlüssel-Verfahren) oder auch Vernam-Chiffre[15] genannte Verfahren ist ebenso einfach wie wenig praxistauglich. Als Schlüssel dient ein be-

11 Jeder wird die entsprechende Vorgehensweise bei dem Kinderspiel „Galgenmännchen“ (auch „Galgenraten“ oder nur „Galgen“ genannt) erinnern.

12 Teilweise wird auch Transposition als Oberbegriff verwendet. Dies ist nicht ganz korrekt, da eine Transposition eine Permutation durch Vertauschen zweier Elemente darstellt. Der Begriff Permutation lässt die Anzahl der vertauschten Elemente dagegen offen und ist damit der richtigerweise zu verwendende Oberbegriff.

13 Vgl. das Beispiel bei *Pohlmann/Hesse,* ITSD 2006, 430, 438 f.

14 Ausführlich dazu *Schneier*, Angewandte Kryptographie, S. 17 ff.

15 Nach seinem Erfinder Gilbert Vernam; *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 59 f.

liebiger Satz Zufallszahlen oder –buchstaben. Dieser Zahlen- oder Buchstabensatz muss mindestens die gleiche Länge aufweisen wie der zu verschlüsselnde Klartext. Klartext und der als Schlüssel dienende Buchstaben- oder Zahlensatz werden dann kombiniert.

Eine Kombinationsmöglichkeit ist etwa die Umwandlung des Klartexts in Zahlen (wobei z.B. A der 1 entsprechen würde, B der 2 usw.) und der folgenden Addition der einzelnen Zahlen des Schlüssels.[16] Es sind aber auch beliebige andere Möglichkeiten der Kombination denkbar.[17] Besondere Bedeutung in der Kryptographie hat die Exklusiv-oder-Verknüpfung (häufig auch nur als `XOR´ bezeichnet[18]), bei der jeweils ein Klartextbit mit einem Schlüsselbit addiert wird. Mögliche Werte sind jeweils nur 0 und 1, woraus sich folgende Kombinationen ergeben:[19]

$$0 \oplus 0 = 1$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

Die Bezeichnung *Einmal*verschlüsselung (`*One-Time*-Pad´) rührt daher, dass der Schlüssel nur *einmal* verwendet werden darf, um die Sicherheit des Verfahrens nicht zu korrumpieren.[20] Wird der aus zufälligen Zahlen oder Zeichen generierte[21] Schlüssel nur ein Mal verwendet, ergibt sich ein Chiffretext, der keinerlei Anhaltspunkte für die Kryptoanalyse und damit für ein Brechen der Verschlüsselung bietet: Bei Kombination eines unbekannten Klartexts mit jeweils einem rein zufällig ausgewählten Zeichen oder einer Zahl ist – auch ohne vertiefte mathematische Kenntnisse – offensichtlich, dass ein solcher Chiffretext ohne Kenntnis des Schlüssels nicht entziffert werden kann.[22]

Dem Vorteil der absoluten Sicherheit stehen in der praktischen Anwendung aber eine Reihe von Nachteilen gegenüber: Für jede zu verschlüsselnde Nachricht muss ein neuer Schlüssel generiert werden. Dieser muss sehr lang sein, mindestens so lang

16 Siehe dazu auch *Schneier*, Secrets and Lies, S. 106.

17 Wikipedia, One-Time-Pad, Version vom 25.02.2008, 09.09 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=One-Time-Pad&oldid=42956062.

18 Siehe *Eckert*, IT-Sicherheit, S. 296 f.; *Schneier*, Angewandte Kryptographie, S. 15 ff.

19 Nach *Schneier*, Angewandte Kryptographie, S. 15.

20 *Schneier*, Secrets and Lies, S. 106; *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 60.

21 Eine tatsächlich zufällige Reihenfolge von Zahlen oder Zeichen kann nicht durch den Anwender erstellt werden, da der Mensch dazu tendiert, nach wahrscheinlichkeitstheorethischen Gesichtspunkten eine in etwa gleichmäßige Verteilung der verwendeten Zahlen oder Zeichen anzustreben. Daraus ergeben sich erleichterte Angriffsmöglichkeiten, das Verschlüsselungsverfahren zu brechen. Eine „echt“ zufällige Verteilung kann in der Regel nur durch Einsatz von entsprechenden Computerprogrammen zur Generierung von Zufallszahlen oder –zeichen erreicht werden. Vgl. *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 147 ff.

22 Vgl. mit Beispielen *Schneier*, Angewandte Kryptographie, S. 18; *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 60.

wie die Nachricht selbst.[23] Dadurch werden Ver- wie Entschlüsselungsvorgang zeit- und ressourcenintensiv. Vor allem aber wird zur Übermittlung des Schlüssels an den Kommunikationspartner bereits ein sicherer, d.h. nicht abhörbarer Übermittlungskanal benötigt. Gibt es keine Möglichkeiten des persönlichen Kontakts zum Schlüsselaustausch, besteht das Dilemma, das durch die Anwendung von Verschlüsselungsverfahren gelöst werden soll, fort:[24] Wie übermittle ich eine Nachricht über unsichere Kanäle, ohne dass ein Dritter vom Inhalt der Nachricht Kenntnis nehmen kann?

II. Moderne Verschlüsselungsverfahren

1. Symmetrische und asymmetrische Verschlüsselungsverfahren

Moderne Verschlüsselungsverfahren haben sich vor allem diesem Problem des Schlüsselaustauschs gewidmet und in den 70er Jahren eine revolutionäre Idee entwickelt: Statt wie bisher zum Ver- und Entschlüsseln denselben Schlüssel zu verwenden (so genannte symmetrische Verschlüsselungsverfahren[25]), wurde jetzt mit zwei Schlüsseln gearbeitet.[26] Bei der so genannten asymmetrischen Verschlüsselung generiert der Anwender Schlüssel*paare*. Ein Schlüssel des Schlüsselpaars wird veröffentlicht (daher auch als öffentlicher Schlüssel bzw. *`public key´* bezeichnet), während der andere Schlüssel des Schlüsselpaars nur dem Anwender bekannt bleibt (der so genannte private Schlüssel oder *`private key´*). Da die Besonderheit der asymmetrischen Kryptographie die Existenz eines öffentlichen, jedermann zugänglichen Schlüssels ist, werden solche Verfahren auch als *`Public Key Kryptographie´* bezeichnet.

Möchte Absender A dem Empfänger B eine verschlüsselte Nachricht übermitteln, benötigt er nur den öffentlichen Schlüssel von B. Mit diesem verschlüsselt A die Nachricht. Allein der Empfänger B verfügt über den zugehörigen privaten Schlüssel zur Entschlüsselung und kann die Nachricht entschlüsseln.

23 Bei Verwendung eines kürzeren Schlüssels müssten die Zeichen oder Zahlen des Schlüssels ganz oder zum Teil mehrfach verwendet werden. Daraus können sich (jedenfalls theoretisch) Anhaltspunkte zum Brechen der Verschlüsselung ergeben.

24 *Schneier*, Secrets and Lies, S. 107; *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 61.

25 Die Bezeichnung als symmetrisch rührt daher, dass das Geheimwissen um den Schlüssel symmetrisch im Sinne von gleichmäßig zwischen den Kommunikationspartnern verteilt ist.

26 In der praktischen Anwendung werden häufig sog. hybride Verschlüsselungsverfahren verwendet, die symmetrische *und* asymmetrische Verschlüsselungsverfahren nutzen, um so von den jeweiligen Vorteilen zu profitieren (symmetrische Verschlüsselungsverfahren sind schneller, asymmetrische Verfahren lösen das Problem des Schlüsselaustauschs). Hybride Verschlüsselungsverfahren sollen etwa bei der elektronischen Gesundheitskarte eingesetzt werden; vgl. Gematik GmbH, Die elektronische Gesundheitskarte: whitepaper Sicherheit, verfügbar unter: http://www.gematik.de/(S(vdkzifron3gqkkysw4nr5jro))/Pressemitteilung___09_05_2008.Gematik (26.10. 2009), S. 11.

2. RSA-Verfahren als Beispiel asymmetrischer Verschlüsselungsverfahren

Eines der ersten derartigen asymmetrischen Verschlüsselungsverfahren ist das so genannte RSA-Verfahren.[27] Das Verfahren wird hier als Beispiel gewählt, weil es nicht nur das erste praktisch bedeutsame Public Key Verfahren war, sondern auch bis heute Anwendung findet.[28]

Das RSA-Verfahren basiert – wie alle anderen Public Key Verfahren auch – auf einer so genannten mathematischen Einwegfunktion (`*one-way function´*). Einwegfunktionen sind Funktionen, die „leicht", d.h. effizient, berechnet werden können, die aber nur „schwer" umkehrbar sind.[29] „Schwer" bedeutet, dass es kein effizientes Verfahren zur Berechnung der Umkehrfunktion gibt.

Für Verschlüsselungsanwendungen ist eine Einwegfunktion mit Falltür (kurz auch nur Falltürfunktion, `*trap door one-way function´*) erforderlich, denn der Empfänger soll mit einer Zusatzinformation (aus dem privaten Schlüssel) die Umkehrfunktion berechnen können.[30]

Die für das RSA-Verfahren verwendete Einwegfunktion mit Falltür basiert auf dem so genannten Faktorisierungsproblem:[31] Es ist effizient möglich, aus zwei großen Primzahlen deren Produkt zu berechnen. Es ist aber nicht effizient möglich, aus dem gegebenen Produkt die beiden Primzahlfaktoren zu berechnen, wenn bei der Wahl der Faktoren bestimmte Vorgaben beachtet werden. Die beiden Primzahlfaktoren dürfen z.B. nicht zu nahe beieinander liegen, da dies einen Angriff durch schlichtes Ausprobieren (sog. `*Brute-Force´*-Angriff oder Exhaustionsmethode)[32]

27 Es wurde nach den Anfangsbuchstaben der Nachnamen seiner Entwickler benannt, den Mathematikern Ronald Rivest, Adi Shamir und Leonard Adleman. Vgl. ausführlich zu diesem Verfahren *Bourseau/Fox/Thiel,* DuD 2002, 84.

28 Bundesamt für Sicherheit in der Informationstechnik, E-Government-Handbuch: Verschlüsselung und Signatur, verfügbar unter: http://www.bsi.de/fachthem/egov/download/2_Krypto.pdf (26.02.2008), S. 4, 20. Die elektronische Gesundheitskarte verwendet derzeit ebenfalls noch RSA mit Schlüssellängen von 2048 Bit. In Zukunft sollen aber auf elliptischen Kurven basierende Verfahren zum Einsatz kommen; vgl. Gematik GmbH, Die elektronische Gesundheitskarte: whitepaper Sicherheit, verfügbar unter: http://www.gematik.de/(S(vdkzifron3gqkkysw4nr5jro))/Pressemitteilung___09_05_2008.Gematik (26.10.2009), S. 143.

29 *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 103.

30 *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 103.

31 Ausführlich dazu Wikipedia, Faktorisierungsverfahren, Version vom 09.06.2009, 14.45 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Faktorisierungsverfahren&oldid=60949714; *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 104 f., 108 f. Ein weiteres für Verschlüsselungsverfahren eingesetztes Problem ist das diskrete Logarithmusproblem, vgl. *Eckert*, IT-Sicherheit, S. 319 f. In letzter Zeit wird dabei verstärkt auf Verfahren gesetzt, die auf elliptischen Kurven basieren, da die Berechnung des diskreten Logarithmus in der Gruppe der Punkte elliptischer Kurven ein äußerst schweres Berechnungsproblem darstellt; vgl. *Eckert*, IT-Sicherheit, S. 332 f. sowie Wikipedia, Elliptic Curve Cryptography, Version vom 15.10.2009, 17.45 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Elliptic_Curve_Cryptography&oldid= 65617819.

32 Derartige Formen von Angriffen bezeichnet man allgemein als `*Brute-Force´*-Methode, `*Brute-Force´*-Angriff (vom engl. brute force – rohe Gewalt) oder auch als Exhaustionsmethode

der Primzahlfaktoren begünstigen würde, den man ausgehend von der Wurzel des Produkts starten könnte.[33]

III. Sicherheit moderner Verschlüsselungsverfahren

1. Relativität der Sicherheit

Das Sicherheitskonzept moderner Verschlüsselungsverfahren basiert *nicht* auf der *Garantie absoluter Sicherheit*, wie dies bei der mathematisch beweisbar sicheren Einmalverschlüsselung (`*One-Time-Pad´*) der Fall ist. Die Sicherheit moderner Verschlüsselungsverfahren beruht im Wesentlichen auf zwei Faktoren: Zeit und Wahrscheinlichkeit.

Verschlüsselungsverfahren nutzen mathematische Einwegfunktionen, für die *bisher* kein effizienter Algorithmus[34] zur Umkehrung der Funktion gefunden wurde. Daher ist (theoretisch) möglich, dass morgen ein solcher effizienter Umkehralgorithmus gefunden wird. Handelt es sich bei der verwendeten Einwegfunktion allerdings um ein bekanntes mathematisches Problem, das mithin schon Gegenstand wissenschaftlicher Auseinandersetzung war, ist es extrem unwahrscheinlich, dass die Funktion „plötzlich" gebrochen wird. Neben der Entdeckung eines effizienten Umkehralgorithmus besteht theoretisch auch die Möglichkeit, dass bei einem `*Brute-Force´*-Angriff auf eine konkrete Verschlüsselung schnell die richtigen Parameter (etwa die beiden Primzahlen im Rahmen des Faktorisierungsproblems) erraten werden.[35] Die Sicherheit von asymmetrischen Verschlüsselungsverfahren beruht darauf, dass dies sehr unwahrscheinlich ist.

Im Übrigen basiert die Sicherheit von Verschlüsselungsverfahren schlicht auf Zeitablauf: Die den Algorithmen zu Grunde liegenden Einwegfunktionen sind *prinzipiell* umkehrbar, sie sind *nur nicht in einer aus Sicht des Angreifers angemessenen Zeitspanne* umkehrbar. Welche Zeitspanne als angemessen angesehen wird, hängt maßgeblich von der Bedeutung der zu entschlüsselnden Information ab. Theoretisch

(vom lat. exhaurire – ausschöpfen); Wikipedia, Brute-Force-Methode, Version vom 09.05.2009, 00.46 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Brute-Force-Methode&oldid=59854971. Siehe zur Vorgehensweise auch *Schneier*, Angewandte Kryptographie, S. 177 ff.

33 Zur RSA-Kryptoanalyse siehe *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 110 ff.

34 „Unter Algorithmen im engeren Sinne versteht man Rechen- bzw. Verarbeitungsvorschriften, die auf eine ganze Klasse von Problemen anwendbar sind und die so präzise festgelegt sind, dass sie ein gegebenes Problem - trotz Schleifen und Verzweigungen - mit endlich vielen Rechenschritten (Finitheit) und regelmäßig bei gleichen Ausgangsbedingungen nur in einer Weise abarbeiten und nur mit einem bestimmten Ergebnis lösen (Determiniertheit)."; *Grützmacher*, in: *Wandtke/Bullinger,* UrhR, § 69a, Rn. 28. Ausführlich zum Begriff des Algorithmus auch *Marly,* Praxishandbuch Softwarerecht, Rn. 29 ff. mit vielen weiteren Nachweisen.

35 *Hartmann*, Sichere Kommunikation im Internet, S. 41.

existiert sogar eine absolute, physikalische Obergrenze, welche Schlüssellängen überhaupt noch entschlüsselt werden können. [36] Selbst bei weiterhin zunehmenden Rechnerkapazitäten wären Verschlüsselungsverfahren, die derart lange Schlüssel verwenden, danach auch in Zukunft sicher. Da einer solchen Betrachtung aber immer nur die bisher bekannten Angriffsstrategien[37] und technologischen Ressourcen[38] zu Grunde liegen, sollte auf das Fortbestehen solcher vermeintlich absoluter Grenzen der Entschlüsselbarkeit nicht vertraut werden.

Quantencomputer als neue Technologie könnten in der Tat erhebliche Auswirkungen auf die Sicherheit von Verschlüsselungsverfahren haben. Allerdings nicht – wie teilweise suggeriert wurde – dergestalt, dass mit der Quantentechnologie schlagartig alle präexistenten Verschlüsselungsverfahren unsicher würden. Zwar würden Quantencomputer einen gigantischen Kapazitätssprung in der Kryptoanalyse bedeuten, der auch mit großen Schlüssellängen arbeitende Verschlüsselungsverfahren unsicher werden ließe. Dies würde aber zum einen nicht so schlagartig geschehen, dass nicht auch Zeit für entsprechende Vorsorgemaßnahmen und Adaption von Schlüssellängen und Verschlüsselungsverfahren wäre.[39] Zum anderen stünden Quantencomputer stets nicht nur der Kryptoanalyse, sondern auch der Kryptographie zur Verfügung. Bereits jetzt ist die Quantentechnologie zumindest so weit fortgeschritten, dass sie für einen sicheren Schlüsseltausch verwendet werden kann.[40] Wegen der exponentiell angestiegenen Kapazitäten wird die – mit bisherigen Verfahren zu aufwändige – Nutzung von Einmalschlüssel-Verfahren (`*One-Time-Pad´*) möglich. Damit steht schon jetzt unter Verwendung von Quantentechnologie ein absolut sicheres Verschlüsselungsverfahren zur Verfügung.[41]

Schließlich wurden in der Vergangenheit entscheidende kryptoanalytische Fortschritte weniger durch neue *technische* Möglichkeiten, als vor allem durch neue oder

36 Diese liegt laut *Schneier*, Angewandte Kryptographie, S.185 bei 256 Bit Schlüssellänge für symmetrische Verfahren.

37 Die Aussage *Schneiers* bezieht sich beispielsweise nur auf die `*Brute-Force´*-Attacke; *Schneier*, Angewandte Kryptographie, S.185.

38 In *Schneiers* Rechnung wurde von konventioneller Computertechnik ausgegangen; *Schneier*, Angewandte Kryptographie, S.185. Die Quantentechnologie könnte hier zu anderen Bewertungsmaßstäben führen.

39 Das Thema Quantencomputer steht bereits seit 15 Jahren auf der Agenda. Fortschritte sind in diesem Bereich erzielt worden, bis zu einem zuverlässigen breiteren Einsatz wird aber noch einige Zeit vergehen; *Hemmer/Wrachtrup,* Science 2009, 473, 473.

40 *Hemmer/Wrachtrup,* Science 2009, 473, 473. Vgl. zum sicheren Schlüsseltausch und Abhörangriffen in der Praxis Zeppmeisel, Quantenkryptographie, verfügbar unter: http://www.cip.physik.uni-muenchen.de/~milq/quantenkryp/Quantenkryptographie.pdf (08.06.2009), S. 85 ff.

41 Dieser sichere Schlüsseltausch von Einmalschlüsseln wird als Quantenkryptographie bezeichnet; Zeppmeisel, Quantenkryptographie, verfügbar unter: http://www.cip.physik.uni-muenchen.de/~milq/quantenkryp/Quantenkryptographie.pdf (08.06.2009), S. 33; Wikipedia, Quantenkryptografie, Version vom 07.04.2009, 08.34 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Quantenkryptografie&oldid=58766300.

verbesserte *mathematische Verfahren* erzielt, mit deren Hilfe der Schlüsselraum eingeschränkt werden konnte.[42]

> „Was bleibt, um Algorithmen zu schwächen, sind mathematische Angriffe. Die einzige Gefahr bei diesen Algorithmen mit großer Schlüssellänge kommt von mathematischer Einsicht. Wenn es jemandem gelingt, wenn er sagt: ‚Ich bin nicht so blöd, dass ich all diese zwei hoch 256 Schlüssel durchsuchen muss, sondern ich kann das auf ganz wenige reduzieren' - darauf kommt es an -, dann besteht eine Gefahr. Das ist die einzige Gefahr, die besteht. Zuwachs von Computerpower ist keine Gefahr, nur mathematische Einsicht."[43]

Das Sicherheitskonzept moderner Verschlüsselungsverfahren kann insoweit als Konzept relativer Sicherheit verstanden werden, mit den Variablen Zeit und Wahrscheinlichkeit. Bei Verwendung entsprechender Schlüssellängen kann die Möglichkeit eines Brechens der Verschlüsselung innerhalb einer adäquaten Zeitspanne allerdings als lediglich theoretisch denkbar, praktisch aber irrelevant qualifiziert werden. Die Abhängigkeit der Sicherheit von Verschlüsselungsverfahren von Wahrscheinlichkeitsbetrachtungen und Zeitfaktor (Relativität) schließt aber die Einordnung moderner asymmetrischer Verschlüsselungsverfahren unter die absolut sicheren Verschlüsselungsverfahren nicht aus: Zwar sind diese Verfahren nicht wie die Einmalverschlüsselung mathematisch beweisbar sicher, sie sind aber *praktisch* sicher:

> „Ein sinnvolles Maß an Sicherheit für ein kryptographisches Verfahren ist dann erreicht, wenn kryptoanalytische Methoden, zu denen auch das Ausprobieren aller möglichen Schlüssel (Brute-Force-Attacke) zählt, nur unter großem Aufwand von Ressourcen (Zeit, Hard- und Software, Personen, Know-how) möglich ist. Für einen externen Angreifer stellt sich immer die Frage nach dem Gegenwert der entschlüsselten Informationen, der oftmals nicht im Verhältnis zum Aufwand für leistungsfähige Hard- und Software steht."[44]

Sicherheit ist stets ein relativer Begriff und wird technisch als „Freiheit von unvertretbaren Risiken"[45] definiert. Sicherheit ist demnach kein feststehender Zustand,

42 Für das Faktorisierungsproblem etwa das sog. „Quadratische Sieb" (Wikipedia, Faktorisierungsverfahren, Version vom 09.06.2009, 14.45 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Faktorisierungsverfahren&oldid=60949714; Einzelheiten zur Funktionsweise des „Quadratischen Siebs" siehe Wikipedia, Quadratisches Sieb, Version vom 12.06.2009, 14.15 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Quadratisches_Sieb&oldid=61076310 sowie ausführlich *Buchmann*, Einführung in die Kryptographie, S. 164 ff.). Daher veröffentlicht die Bundesnetzagentur auch regelmäßig eine Übersicht über geeignete Algorithmen; zuletzt in der „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung" vom 17.12.2007, verfügbar unter: http://www .bundesnetzagentur.de/media/archive/12198.pdf (14.05. 2008).

43 *Beutelspacher*, Ist Kryptographie gut - oder zu gut?, in: *Hamm/Möller,* Datenschutz durch Kryptographie, S. 16, 37.

44 *Raepple*, Sicherheitskonzepte für das Internet, S. 137.

45 Definition nach DIN EN 61508-4 (VDE 0803 Teil 4): 2002-08: Funktionale Sicherheit elektrischer/elektronischer/programmierbar elektronischer sicherheitsbezogener Systeme – Teil 4: Begriffe und Abkürzungen, Berlin 2002, Ziffer 3.1.8 sowie nach ISO/IEC Guide 51:1999: Safety aspects -- Guidelines for their inclusion in standards, Definition 3.1, zitiert nach: Voges, Definitionen von Begriffen im Kontext ‚Sicherheit (safety)', Vortrag im Rahmen des GI-Workshop zum fachlichen Zusammenhang der Fachgruppen im neuen Fachbereich "Sicher-

sondern wird stets in Abhängigkeit vom Vorliegen von Risiken bestimmt. Sicherheit ist also per se keine absolute Größe, sondern eine relative:[46]

> „Security is never black and white, and context matters more than technology. […] A system might be secure as long as certain mathematical advances don´t occur, or for a certain period of time, or against certain types of attacks. Like any adjective, 'secure' is meaningless out of context."[47]

Dies gilt auch für das beweisbar absolut sichere Einmalschlüssel-Verfahren. Die Aussage der mathematisch beweisbaren, absoluten Sicherheit bezieht sich allein auf den Algorithmus. Ein Verschlüsselungsverfahren im praktischen Einsatz besteht aber nicht nur aus dem zu Grunde liegenden Algorithmus, sondern auch aus der konkreten Implementierung, der Sicherheit des gesamten informationstechnischen Systems, auf dem das Verschlüsselungsverfahren verwendet wird, der Sicherheit verwendeter Passwörter etc.[48]

> „Die heutigen Algorithmen, auch DES[49], Triple-DES, IDEA, RSA mit der entsprechenden Schlüssellänge, sind so sicher, dass das ganz bestimmt nicht der wunde Punkt an einem Sicherheitssystem ist. Wenn ich gefragt würde, wie man ein Sicherheitssystem angreift, würde ich bestimmt nicht sagen, zuerst den Algorithmus knacken. Es gibt in der Regel viel, viel weichere Stellen."[50]

Die Sicherheit eines Verschlüsselungsverfahrens als Ganzem ist daher stets relativ. Werden jedoch bei der gesamten Implementierung und Anwendung eines Verschlüsselungsverfahrens keine Schwachstellen geschaffen, die sich für einen Angriff ausnutzen lassen, dann gewährleisten Verschlüsselungsalgorithmen absolute Sicherheit der Vertraulichkeit von Daten.

> „Wenn der zum Aufbrechen eines Algorithmus erforderliche Geldaufwand den Wert der verschlüsselten Daten übersteigt, sind Sie wahrscheinlich sicher. Wenn die dafür notwendige Zeit größer ist als die Zeitspanne, die die verschlüsselten Daten geheim bleiben müssen, sind Sie wahrscheinlich sicher. Wenn das mit einem bestimmten Schlüssel chiffrierte Datenvolumen kleiner ist als die Datenmenge, die zum Knacken des Algorithmus erforderlich ist, sind Sie wahrscheinlich sicher. Ich sage `wahrscheinlich´, da immer mit der Möglichkeit neuer Durchbrüche in der Kryptanalyse zu rechnen ist. Demgegenüber nimmt der Wert der meisten Daten mit der Zeit ab. Es ist wichtig, dass der Wert der Daten immer unter den Kosten liegt, die zum Durchbrechen der entsprechenden Sicherheitsvorkehrungen erforderlich sind.“[51]

heit" am 12.02.2002, verfügbar unter: http://www11.informatik.uni-erlangen.de/Aktuelles/Veranstaltungen/Sicherheit1/PositionPapers/Voges.pdf (13.02.2008).

46 So auch Bundesamt für Sicherheit in der Informationstechnik, IT-Sicherheitshandbuch, verfügbar unter: http:// www.bsi.de/literat/kriterie.htm (13.2.2008), Kap. 2.3.

47 *Schneier*, Secrets and Lies, S. 13.

48 *Hartmann*, Sichere Kommunikation im Internet, S. 40 f.; siehe ausführlich zur Sicherheit von Passwörtern *Schneier*, Secrets and Lies, S. 138 ff.

49 DES (`*Data Encryption Standard´*), Triple-DES (eine Weiterentwicklung des DES) und IDEA (`*International Data Encryption Algorithm´*) sind Verschlüsselungsalgorithmen.

50 *Beutelspacher*, Ist Kryptographie gut - oder zu gut?, in: *Hamm/Möller,* Datenschutz durch Kryptographie, S. 16, 37.

51 *Schneier*, Angewandte Kryptographie, S. 9.

2. „Absolute Sicherheit“ von Verschlüsselungsverfahren

Soweit hier[52] Verschlüsselungsverfahren als „absolut sicher“ bezeichnet werden, ist dies weniger als Gegenstück (und damit Widerspruch) zur Relativität von Sicherheit zu verstehen, sondern als Referenz an die Allumfassendheit dieser Sicherheit:[53] Verschlüsselungsverfahren verhindern *umfassend* die Kenntnisnahme Dritter, unabhängig ob es sich um kriminelle Angriffe handelt oder richterlich genehmigte Ermittlungsmaßnahmen staatlicher Sicherheitsbehörden. Dies unterscheidet Verschlüsselungsverfahren wesentlich von sonstigen (technischen) Verfahren. Die klassische Telekommunikation und die Post sind auch auf die Sicherung der Vertraulichkeit der übermittelten Kommunikation angelegt. Die Sicherungsmaßnahmen richten sich aber gegen unbefugte Dritte; der Staat kann jederzeit (bei Vorliegen der gesetzlichen Voraussetzungen) Briefverkehr und Telekommunikation überwachen. Verschlüsselungsverfahren können hingegen nicht beides gewährleisten: Sie können entweder sicher sein – dann verhindern sie effektiv die Kenntnisnahme Dritter, unabhängig von der Identität des Dritten und des Zweckes der Kenntnisnahme. Oder sie können unsicher sein – dann gewähren sie auch gegenüber niemandem Kommunikationsvertraulichkeit.[54]

IV. Digitale Signatur als weiterer Einsatzbereich von Verschlüsselung

Die Prinzipien der Public Key Kryptographie liegen auch der so genannten digitalen Signatur[55] zu Grunde – allerdings in genau umgekehrter Verwendung der Schlüssel:

52 Informationstechnisch ist natürlich nur die mathematisch beweisbar sichere Einmalverschlüsselung `absolut sicher´, andere Verschlüsselungsverfahren sind `praktisch´ oder `wahrscheinlich´ sicher; *Eckert*, IT-Sicherheit, S. 286 ff.; *Schneier*, Angewandte Kryptographie, S. 9 f., 275.

53 Und insoweit steht dies auch der von *Dix,* CR 1997, 38, 43 vertretenen Auffassung, es gebe keine absolut sicheren Verschlüsselungsverfahren, nicht entgegen. Denn Dix bezieht sich auf die ständig steigende Rechnerkapazität und die daraus resultierende Notwendigkeit zur kontinuierlichen Verbesserung und Weiterentwicklung von Verschlüsselungsverfahren. Seine Aussage „Schon begrifflich gibt es keine absolut sicheren Verschlüsselungsverfahren“ (ebenda) ist mit Blick auf das `*One-Time-Pad*´ schlicht falsch. In der Sache dürfte sich Dix auf die bereits dargestellten Phänomene der Angreifbarkeit und des Unsicherwerdens von Verschlüsselungsverfahren beziehen.

54 Solche Verfahren können allein die *zufällige* Kenntnisnahme verhindern, so wie ein Briefumschlag die zufällige Kenntnisnahme verhindert im Gegensatz zur Postkarte. Jeder interessierte Dritte, der mithin bereit ist, gewisse Ressourcen aufzubieten, um bestimmte Kommunikation zu entschlüsseln, kann dagegen Kenntnis nehmen.

55 Mit dem Begriff der „digitalen Signatur“ wird allein auf das *technische* Verfahren Bezug genommen. Der vielfach ebenso verwendete Begriff der „elektronischen Signatur“ ist dagegen ein *Rechts*begriff (vgl. § 2 Nr. 1-3 SigG), der durch eine digitale Signatur umgesetzt werden kann (so etwa bei einer fortgeschrittenen oder einer qualifizierten Signatur gem. § 2 Nr. 2 bzw. 3 SigG), aber nicht zwingend durch eine digitale Signatur umgesetzt werden muss (im Falle der einfachen elektronischen Signatur nach § 2 Nr. 1 SigG); dazu *Benesch,* JurPC 24/

Verschlüsselungsverfahren halten zwar den Inhalt einer E-Mail (oder sonstiger Daten[56]) vertraulich, gewährleisten aber weder, dass die E-Mail tatsächlich von demjenigen herrührt, der als Absender erscheint, noch, dass die E-Mail bei der Übermittlung nicht verändert wurde (Integrität der Daten[57]). Dem dient die digitale Signatur.

1. Zusammenhang von Verschlüsselung und digitaler Signatur

Die digitale Signatur verwendet auch Verschlüsselungsverfahren, gewährleistet aber nicht die Vertraulichkeit von Daten, sondern allein die Integrität von Daten.[58] *Wer sowohl die Vertraulichkeit als auch die Integrität von Daten sicherstellen will, muss diese Daten sowohl verschlüsseln als auch digital signieren.* Sowohl die Verschlüsselung zur Gewährleistung von Vertraulichkeit als auch die digitale Signatur zur Gewährleistung der Integrität basieren technisch auf Verschlüsselungsverfahren, verwirklichen aber unterschiedliche Schutzziele. Hier wird im Folgenden nur der isolierte Einsatz von Verschlüsselungsverfahren im Rahmen der digitalen Signatur zur Gewährleistung der Integrität von Daten dargestellt. In der Praxis werden Daten, deren Integrität durch eine digitale Signatur sichergestellt wird, sicher regelmäßig auch vertraulich bleiben sollen, so dass die Daten zusätzlich verschlüsselt werden. Um das Verständnis zu erleichtern, wird hier allein die Funktionsweise der digitalen Signatur erläutert.

2. Funktionsweise der digitalen Signatur

Verwendet werden dazu Public Key Verfahren wie das RSA-Verfahren, dem bis heute bekanntesten und meistgenutzten Verfahren für digitale Signaturen.[59] Zur Erzeugung einer digitalen Signatur werden die beiden Schlüssel in umgekehrter Weise eingesetzt: Der Absender A einer Nachricht *verschlüsselt* diese Nachricht *mit seinem privaten Schlüssel*. Der Empfänger B *entschlüsselt* die Nachricht *mit dem zugehörigen öffentlichen Schlüssel des Absenders A*. Somit weiß B, dass die Nachricht von A stammt, da er sie ansonsten nicht mit dem öffentlichen Schlüssel des A (sinnvoll)

2002, Rn. 9; Wikipedia, Digitale Signatur, Version vom 21.03.2009, 23.54 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Digitale_Signatur&oldid=58169161. Vgl. zur Funktionsweise auch *Soergel/Marly*, BGB, § 126a, Rn. 8 f. m.w.N.

56 Die E-Mail ist insoweit hier nur als Beispiel zu verstehen.

57 Die Gewährleistung, dass eine E-Mail tatsächlich von demjenigen herrührt, der als Absender erscheint, wird auch als Authentizität bezeichnet. Der Begriff wurde hier nicht verwendet, da nach dem hier vertretenen Verständnis Authentizität stets Voraussetzung und daher Teil des Schutzziels der Integrität von Daten ist. Vgl. ausführlich dazu unter B.III.1.a.bb).

58 Integrität umfasst nach hier vertretener Auffassung auch die Authentizität; siehe unter B.III.1.a.bb).

59 So Wikipedia, Digitale Signatur, Version vom 21.03.2009, 23.54 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Digitale_Signatur&oldid=58169161.

hätte entschlüsseln können. B weiß auch, dass die Daten nicht verändert wurden. Dazu müsste ein Angreifer in der Lage sein, die Daten so zu verändern, dass sich bei der Entschlüsselung ein anderer, ebenfalls sinnvoller Text ergibt. Da ein Brechen der Verschlüsselung innerhalb einer adäquaten Zeitspanne ausgeschlossen ist (s.o. unter III.1.), ist dies praktisch unmöglich.

3. Hashwerte

Signaturverfahren verwenden in der Regel so genannte Hashwerte, um die Vorgänge des Signierens wie der Signaturprüfung schneller durchführen zu können.[60] Das Verschlüsseln aller zu signierender Daten mit dem privaten Schlüssel des Absenders ist ressourcen- und damit unter Umständen auch zeitintensiv. Daher werden in der Regel Prüfsummen der zu signierenden Daten gebildet und nur diese werden signiert. Hashfunktionen stellen eine Option zur Erzeugung von Prüfsummen mit einem hohen Sicherheitsniveau dar.[61] Die derart generierten Prüfsummen werden Hashwerte genannt und zum Teil mit dem menschlichen Fingerabdruck verglichen (daher sind auch die Bezeichnungen `*Fingerprint´* oder `digitaler Fingerabdruck´[62] für Hashfunktionen geläufig)[63]: So wie Menschen nahezu eindeutig durch ihre Fingerabdrücke identifiziert werden können, stellt ein Hashwert eine nahezu eindeutige Kennzeichnung einer größeren Datenmenge dar.

Jedes Objekt (z.B. eine Datei) kann mittels einer Hashfunktion auf einen viel kleineren Hashwert abgebildet werden. Dazu wird in der Regel eine Folge von gleichartigen Kompressionsfunktionen eingesetzt.[64] Sichere Hashfunktionen müssen zum einen Einweg-Funktionen sein, wie sie auch für moderne Verschlüsselungsverfahren eingesetzt werden. Eine Einweg-Funktion ist eine Funktion, bei der der Funktionswert „leicht“, d.h. vor allem schnell, berechnet werden kann, die Berechnung einer Umkehrung des Funktionswertes aber nur „schwer“ möglich ist, d.h. vor allem lange dauert (Einweg-Eigenschaft).[65] Sichere Hashfunktionen müssen irreversibel sein. Es muss unmöglich sein, aus dem Hashwert die diesem Hashwert zu Grunde liegende Eingabe zu ermitteln.

60 Siehe ausführlich dazu *Soergel/Marly*, BGB, § 126a, Rn. 9 m.w.N.

61 Vgl. zu anderen Prüfsummenverfahren Wikipedia, Prüfsumme, Version vom 10.03.2010, 19.30 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Pr%C3%BCfsumme&oldid=71706214.

62 *Eckert*, IT-Sicherheit, S. 345.

63 Wikipedia, Hashfunktion, Version vom 16.04.2009, 00.46 Uhr, verfügbar unter: http://de.wikipedia.org/w/inde x.php?title=Hashfunktion&oldid=59070874.

64 *Eckert*, IT-Sicherheit, S. 350.

65 Wikipedia, Einwegfunktion, Version vom 02.10.2008, 22.27 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?oldid=51406109; Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, M 3.23 Einführung in kryptographische Grundbegriffe, verfügbar unter: http://www.bsi.bund.de/gshb/deutsch/m/ m03023.htm (07.01.2009).

Da ein viel größeres Dokument auf einen erheblich kleineren Hashwert abgebildet wird, kann es grundsätzlich zu Kollisionen kommen; das bedeutet, zwei unterschiedliche Datensätze können denselben Hashwert haben.[66] Eine sichere, starke Hashfunktion erfordert daher zum anderen, dass es *praktisch nicht möglich sein darf*, zwei verschiedene Eingabewerte *zu finden*, deren Hashwerte übereinstimmen (sog. Kollisionsresistenz).[67] Dies wird über die Länge des Hashwerts sichergestellt.[68]

Beim Versand einer E-Mail wird nur der Hashwert der Daten mit dem privaten Schlüssel des Absenders verschlüsselt und nicht mehr die Daten selbst. Der verschlüsselte Hashwert und die vollständige Nachricht im Klartext[69] werden gemeinsam versandt. Der Empfänger der Daten bildet aus der Klartext-Nachricht ebenfalls den Hashwert: stimmt dieser Hashwert mit dem (mit dem öffentlichen Schlüssel des Absenders) entschlüsselten Hashwert überein, steht fest, dass die Daten bei der Übertragung nicht manipuliert wurden.

Hinsichtlich der Sicherheit digitaler Signaturverfahren gelten dieselben Grundsätze wie bei modernen asymmetrischen Verschlüsselungsverfahren, da digitale Signaturverfahren auf diesen modernen Verschlüsselungsverfahren beruhen.[70]

B. Bedeutung von Verschlüsselungsverfahren – eine technische Perspektive

Die Bedeutung von Verschlüsselungsverfahren beruht historisch auf dem Interesse an vertraulicher Kommunikation. Diese Bedeutung von Vertraulichkeit existiert aber nicht nur fort, sie hat durch den gesellschaftlichen Wandel der Informations- und Kommunikationswege signifikanten Zuwachs erfahren.

66 *Eckert*, IT-Sicherheit, S. 346.

67 *Eckert*, IT-Sicherheit, S. 349; Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, M 3.23 Einführung in kryptographische Grundbegriffe, verfügbar unter: http://www.bsi.bund.de/gshb/deutsch/m/m03023.htm (07.01.2009).

68 Die derzeitige Standardlänge liegt bei 160 Bit.

69 Selbstverständlich kann der Nachrichtentext auch verschlüsselt (mit dem öffentlichen Schlüssel des Empfängers!) versandt werden. Hier wird aber nur die Funktionsweise der digitalen Signatur erläutert. Diese will keine Vertraulichkeit sicherstellen. Zur angestrebten Integritätsgewährleistung ist eine Geheimhaltung der übermittelten Nachricht nicht erforderlich. In der Praxis werden in der Regel beide Schutzziele verfolgt und Verschlüsselung und digitale Signatur kombiniert eingesetzt; s.o. unter 1.

70 *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 124. Die im Einzelnen möglichen Angriffe können aber durchaus unterschiedlich sein. Ein Überblick über Angriffe auf Signaturverfahren siehe bei *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 124 f.

I. Verschlüsselung als Maßnahme der Vertraulichkeitssicherung

1. Mangelnder technischer Schutz der Vertraulichkeit in der digitalen Welt

Die Vertraulichkeit von Kommunikation wird in der digitalen Welt nicht gewährleistet. Bedingt durch die Technik der Datenübertragung im Internet (a.) existieren in einer technischen Perspektive weder Vertraulichkeit von Kommunikationsinhalten (b.) noch von Kommunikationsumständen (c.).

a. Technik der Datenübertragung im Internet

Das Internet ist ein weltweites Netzwerk aus Rechnernetzwerken.[71] Der Datenaustausch zwischen einzelnen Rechnern in diesem Netzwerk der Netzwerke erfolgt auf der Basis von Internetprotokollen.[72] Eines der bekanntesten dieser Protokolle ist das `*Transmission Control Protocol/Internet Protocol*´ (TCP/IP).[73] Die Übertragung von E-Mails wird durch das `*Simple Mail Transfer Protocol*´(SMTP)[74] gesteuert.[75] Es handelt sich aber nur um zwei Beispiele der etwa 500 Netzwerkprotokolle, auf denen die Netzkommunikation im Internet basiert.[76] Welche Protokolle dabei wie ein-

71 Daher auch der Name `Internet´, der verkürzt für das englische `*interconnected networks*´ steht; Wikipedia, Internet, Version vom 13.04.2009, 15.27 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Internet&oldid=58978408. Eine Definition des Begriffs `Internet´ enthält RFC 4949: Internet Security Glossary, Version 2 vom August 2007, verfügbar unter http://www.heise.de/netze/rfc/rfcs/rfc4949.shtml (29.05.2009), S. 156: "The Internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the IAB (RFC 2026) and (b) the name and address spaces managed by the ICANN."

72 Vgl. insgesamt zur Datenübermittlung im Internet Wikipedia, Internet, Version vom 13.04.2009, 15.27 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Internet&oldid=58978408.

73 Siehe dazu Wikipedia, Transmission Control Protocol/Internet Protocol, Version vom 09.04.2009, 10.10 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Transmission_Control_Protocol/Internet_Protocol& oldid=58841355. Zum `*Internet Protocol*´ siehe *Brands*, IT-Sicherheitsmanagement, S. 20 f.

74 Wikipedia, Simple Mail Transfer Protocol, Version vom 13.04.2009, 15.45 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Simple_Mail_Transfer_Protocol&oldid=58979007.

75 Siehe ausführlich zur technischen Funktionsweise der E-Mail-Übermittlung *Brunst*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, S. 63 ff.

76 Daher bezeichnet man sie auch als Internetprotokollfamilie; vgl. Wikipedia, Internetprotokollfamilie, Version vom 09.04.2009, 10.42 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Internetprotokollfamilie&oldid=58842111; *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 25.

zusetzen und zu konfigurieren sind, ist international standardisiert und in so genannten `*Requests for Comments´*(RFCs) beschrieben.[77]

Technisch werden durch das Zusammenspiel der einzelnen Protokolle der Internetprotokollfamilie die zu übermittelnden Daten zunächst in Datenpakete (IP-Pakete, genauer `*Internet Protocol Datagrams´*[78]) aufgeteilt. Die einzelnen Datenpakete werden getrennt voneinander übermittelt und beim Empfänger wieder in der festgelegten Reihenfolge zusammengesetzt. Dabei ist - im Hinblick auf die Netzwerkstruktur des Internets - kein fester Übermittlungsweg vorgegeben. Welche und wie viele Rechner, Staaten und Jurisdiktionen eine E-Mail durchquert auf ihrem Weg vom Sender zum Empfänger ist weder abseh- noch (technisch) steuerbar.

Die Adressierung der Datenpakete erfolgt allein über die IP-Adresse (`*Internet Protocol´*-Adresse) des Empfängers.[79] *Jeder einzelne Rechner kann dabei weltweit eindeutig durch die ihm zugeordnete IP-Adresse identifiziert werden.*[80] Zuständig für die Vergabe von IP-Adressen ist in Europa, Zentralasien und dem Nahen Osten das `*Réseaux IP Européens Network Coordination Centre´*(RIPE NCC)[81], eine der

77 Vgl. zu Entstehungsgeschichte und Funktionsweise von RFCs Wikipedia, Request for Comments, Version vom 07.04.2009, 10.46 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Request_for_Comments&oldid=58769523.

78 Wikipedia, IP-Paket, Version vom 13.03.2009, 18.50 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=IP-Paket&oldid=57835545.

79 Umfassend dazu Wikipedia, IP-Adresse, Version vom 14.04.2009, 13.18 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=IP-Adresse&oldid=59011060.

80 Häufig stehen aber hinter einem Rechner, der mit einer ihm zugeordneten IP-Adresse eindeutig identifiziert werden kann, *mehrere* weitere Rechner: Zum einen können sich auf Seiten der Endnutzer *mehere* Nutzer mit mehreren Rechnern *einen* Internetzugang und damit eine IP-Adresse teilen (lokales Subnetz). Zum anderen können auf Seiten der Provider IP-Adressen geteilt werden, d.h. dass *eine* IP-Adresse an *mehrere* Rechner vergeben wird (im Hinblick auf die zunehmend knapp werdenden IPv4-Adressen). Dies wird technisch durch eine Unterscheidung von öffentlichem Netz (Internet) einerseits und lokalem Netz (bestehend aus mehreren Rechnern, die sich eine IP-Adresse teilen) andererseits umgesetzt. Die Datenpakete werden jeweils über IP-Adressen adressiert – nur dass innerhalb des lokalen Netzes eigene IP-Adressen vergeben werden, die nicht mit der im öffentlichen Netz verwendeten IP-Adresse übereinstimmen. Sog. `*Network Address Translation´*-Verfahren (NAT) übersetzen jeweils die IP-Adressinformationen von öffentlichem und privatem Netz. Siehe ausführlich dazu Wikipedia, Network Address Translation, Version vom 12.03.2010, 12.10 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Network_Address_Translation&oldid=71685948; Walker, Das Internet: Ein historischer Fehler, verfügbar unter: http://www.heise.de/tp/r4/artikel/16/16648/1.html (30.03.2010). Auch wenn so mehrere Netze und Adressierungen hintereinander geschaltet sind, ändert dies nichts daran, dass eine absolut eindeutige Identifizierbarkeit von Rechnern erforderlich ist – da Datenpakete sonst nicht korrekt adressiert und geroutet werden können. Diese eindeutige Identifizierbarkeit ist bei der Schaffung von Subnetzen mit eigener IP-Adressierung zwar nicht mehr für jeden gegeben, die Eindeutigkeit ist aber nach wie vor vorhanden und muss dies aus technischem Gründen auch sein. Eine weitere Möglichkeit der IP-Adressteilung ist die Zuweisung nur bestimmter Ports. Auch in diesem Fall bleibt es bei der eindeutigen Identifizierbarkeit der einzelnen Rechner.

81 Siehe Wikipedia, RIPE Network Coordination Centre, Version vom 08.09.2009, 12.50 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=RIPE_Network_Coordination_Centre&oldid=64284028.

ICANN (`*Internet Corporation for Assigned Names and Numbers´*) untergeordnete Non-Profit-Organisation. Das RIPE NCC als sog. `*Regional Internet Registry´* vergibt ganze Bereiche von IP-Adressen an sog. `*Local Internet Registries´*. Jede Organisation mit Sitz im Zuständigkeitsbereich des RIPE NCC kann eine solche `*Local Internet Registry´* werden. Vor allem Internet Service Provider, Telekommunikationsunternehmen sowie akademische Institutionen übernehmen diese Funktion.[82] Die `*Local Internet Registries´* vergeben die IP-Adressen dann an den Endnutzer[83] – entweder als dynamische oder als statische IP-Adresse.[84] Nach dem derzeit (noch) hauptsächlich im Internet anzutreffenden IPv4-Standard besteht eine IP-Adresse aus vier Zahlen (jeweils mit Werten zwischen 0 und 255), die durch Punkte voneinander getrennt sind, z.B.

130.83.209.115[85]

Die einzelnen Datenpakete werden auf ihrem Weg vom Sender zum Empfänger durch so genannte *Router* übermittelt. Diese Vermittlungsrechner speichern die Datenpakete temporär und leiten sie dann weiter (`*store-and-forward´*-Prinzip).[86] Dabei „entscheiden" die teilweise auch als „Poststellen" bezeichneten[87] Router auf der Basis von Routingtabellen,[88] wohin ein Datenpaket weitergeleitet wird. Der Übermittlungsweg, den ein Datenpaket auf seinem Weg vom Sender zum Empfänger durch das Internet zurücklegt, wird in einem rein technischen Ansatz allein durch die zu Grunde liegenden Protokolle und Tabellen determiniert. Die Protokolle sind dabei vor allem auf Ausfallsicherheit und Schnelligkeit angelegt – und nicht auf Datenschutz.[89]

82 Vgl. dazu http://www.ripe.net/info/faq/rs/ipv4.html#1 (21.09.2009).

83 Möchte man also herausfinden, welchem Nutzer zu einem bestimmten Zeitpunkt eine bestimmte IP-Adresse zugeordnet war, kann man über die Whois-Abfrage via Internet beim RIPE NCC herausfinden, welcher `*Local Internet Registry´* die IP-Adresse zugeordnet ist. Die `*Local Internet Registry´* kann dann aus den Bestandsdaten ihrer Kunden bzw. aus den Logdateien ersehen, wem die IP-Adresse im betreffenden Zeitpunkt zugewiesen war.

84 Im Falle der dauerhaften Zuordnung einer IP-Adresse spricht man von einer statischen IP-Adresse. Bei der zeitlich begrenzten Zuordnung einer IP-Adresse an einen bestimmten Nutzer (in der Regel für die Dauer einer Sitzung), wird von einer dynamischen IP-Adresse gesprochen. Vgl. ausführlich zur Adressierung *Brunst*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, S. 51 ff.

85 Es handelt sich um eine IP des Hochschulrechenzentrums (hrz) der TU Darmstadt. Der gesamte Adressraum von 130.83.0.0 bis 130.83.255.255 ist an das hrz der TU Darmstadt vergeben.

86 *Eckert*, IT-Sicherheit, S.145.

87 Wikipedia, IP-Adresse, Version vom 14.04.2009, 13.18 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=IP-Adresse&oldid=59011060; *Holznagel*, Recht der IT-Sicherheit, S. 18 vergleicht die Router mit Briefverteilzentren.

88 Die Routingtabelle enthält Informationen über den bestmöglichen (d.h. in der Regel den kürzesten) Weg und teilweise auch alternative Wege zu bestimmten Netzen. Routingprotokolle halten die Tabellen aktuell, so dass etwa auf ausgefallene Verbindungen reagiert werden kann. Vgl. ausführlich zum Routing Wikipedia, Routing, Version vom 10.03.2009, 19.17 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Routing&oldid=57708185.

89 Siehe ausführlich *Braun*, InfSpekt 2010, 201, 202 ff.

b. Technikbedingt fehlende Vertraulichkeit von Kommunikationsinhalten in der digitalen Welt

aa) E-Mail-Kommunikation als paradigmatisches Beispiel fehlender Vertraulichkeit

Diese Konzeption und Implementierung von Datenübertragungen im Internet hat weitreichende Konsequenzen;[90] plakativ ausgedrückt:

Jeder Interessierte kann E-Mails abfangen und lesen.[91]

Die E-Mail wurde hier als Beispiel herausgegriffen, da es sich um den meistgenutzten Internet-Dienst[92] handelt und sich Fragen des Schutzes moderner Kommunikationsformen durch das Fernmeldegeheimnis (Art. 10 I GG) daher schwerpunktmäßig mit E-Mail-Kommunikation befassen. Grundsätzlich gilt das Gesagte aber für sämtliche Kommunikationsinhalte, die in Netzwerken übertragen werden. Die Ansatzpunkte für einen solchen Angriff sind vielfältig, da alle Daten im Internet grundsätzlich im Klartext übertragen werden;[93] folgende Szenarien sind etwa denkbar:[94]

90 Hier wird nur auf die Konsequenzen der Architektur des Internet eingegangen, die für die im Rahmen dieser Arbeit diskutierten Fragen Relevanz haben.

91 Je nach Angriff bedarf es dazu fast keiner besonderen informationstechnologischen Kenntnisse; vgl. etwa den unter (1) sogleich beschriebenen Angriff. Jedenfalls verbreitet sich zunehmend das Geschäftsmodell *`Malware as a Service´*, so dass entsprechende bedienerfreundliche Baukästen und Programme käuflich via Internet erworben werden können: „Um andere Leute auszuspionieren und ihnen ihre Daten zu stehlen, bedarf es mittlerweile keiner Fachkenntnis mehr […]“ (heise online vom 10.06.2008, Trojanerbaukasten mit Rund-um-die-Uhr-Support und Austausch-Service, verfügbar unter: http://www.heise.de/newsticker/Trojanerbaukasten-mit-Rund-um-die-Uhr-Support-und-Austausch-Service--/meldung/109254 (11.06.2008)). Siehe nur den in der genannten heise online-Meldung vorgestellten Baukasten: „Von solch einem Support kann der normale Anwender nur träumen: Rund-um-die-Uhr-Online-Support, 6 Monate lang Softwareersatz, so oft man will. Die Entwickler des Trojanerbaukastens Turkojan bieten ihren Kunden einiges, um sie zufriedenzustellen. In der Gold Edition hat der Kunde laut Preisliste innerhalb von sechs Monaten beliebig oft Anspruch auf eine Ersatzversion des Toolkits, sobald ein Virenscanner einen von ihm gebauten Trojaner erkennt. Daneben wartet die 249 US-Dollar kostende Gold Edition mit zahlreichen Funktionen auf, die weit über das hinausgehen, was man früher von solchen Baukästen gewohnt war: Videostreaming über eine Webcam, Audiostreaming über ein am PC angeschlossenes Mikrofon und Realtime-Screen-Viewing, um jede Aktion auf einem infizierten System verfolgen zu können. Dass ein mit Turkojan 4.0 erstellter Trojaner daneben auch Passwörter ausspähen kann und Tastatureingaben mitliest, muss man da kaum noch erwähnen.“ (heise online, ebda).

92 Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2009, verfügbar unter: http://www.bsi.bund.de/literat/lagebericht/Lagebericht2009.pdf (09.03.2009), S. 11.

93 *Hartmann*, Sichere Kommunikation im Internet, S. 62; *Gassen*, Digitale Signaturen in der Praxis, S. 8.

94 Ausführlich dazu auch *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 29 ff.

(1) Angriffe in `*Local Area Networks´* (LANs)

In lokalen Netzwerken (`*Local Area Networks´*, LANs) werden die Datenpakete oft im Rundfunkmodus (`*Broadcast Routing´*[95]) über das ganze LAN gesendet.[96] Jeder, der Zugriff auf dieses Netzwerk hat, kann leicht alle Daten und Passwörter (!) durch den Einsatz entsprechender sog. `*Sniffer´*-Programme[97] (die via Internet für jedermann zugänglich sind)[98] mitlesen.[99] Aber auch jenseits des `*Broadcast Routing´* kann der gesamte Netzwerkverkehr stets von allen, die Zugriff auf das Netzwerk haben, mitgelesen werden. Dies erfordert allerdings kompliziertere Angriffe,[100] mithin ausgereiftere Kenntnisse des Angreifers. Festzuhalten bleibt, dass ein Mitlesen des gesamten Netzwerksverkehrs in lokalen Netzwerken stets allen Personen möglich ist, die Zugriff auf das Netzwerk haben.

(2) Angriffe in `*Wireless Local Area Networks´* (WLANs)

Bei drahtlosen lokalen Netzwerken (`*Wireless Local Area Networks´*, WLANs) ist für das Mitlesen von Datenpaketen noch nicht einmal ein physischer Zugriff auf das

95 *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 31; Wikipedia, Routing, Version vom 10.03.2009, 19.17 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Routing&oldid=57708185.

96 Abhängig davon, ob die einzelnen Rechner innerhalb des Netzwerks physisch über `*Hubs´* oder über `*Switches´* miteinander verbunden sind (siehe zu den Begriffen und den jeweiligen Vor- und Nachteilen Wikipedia, Hub (Netzwerk), Version vom 29.05.2009, 09.35 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Hub_(Netzwerk)&oldid=60547257 und Wikipedia, Switch (Computertechnik), Version vom 04.06.2009, 11.37 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Switch_(Computertechnik)&oldid=60763765).

97 Vgl. Wikipedia, Sniffer, Version vom 25.03.2010, 15.06 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Sniffer&oldid=72339255.

98 Derartige Software gehört zudem zum unverzichtbaren Werkzeug eines jeden Administrators (*Künnemann,* JurPC 62/2009, Rn. 10), da die Analyse des Netzwerksverkehrs auch der Fehlerdiagnose, Datenfilterung und Entdeckung von Eindringungsversuchen dient.

99 Beispiel nach *Schwenk*, Sicherheit und Kryptographie im Internet, S. 4. S. auch *Eckert*, IT-Sicherheit, S. 88 f. Der Einsatz von `*Sniffer´*-Programmen ist einer der Angriffe, der tatsächlich nahezu jedem Interessierten offen steht, da entsprechende Programme (etwa „Wireshark", Einzelheiten siehe bei Wikipedia, Wireshark, Version vom 05.04.2010, 17.01 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Wireshark&oldid=72779393) kostenlos via Internet erhältlich sind. Das weit verbreitete Programm „Wireshark" etwa ist einfach zu installieren und dürfte von nahezu jedem bedient werden können – zumal etliche Schritt-für-Schritt-Anleitungen mit entsprechenden Screenshots im Internet verfügbar sind; vgl. insoweit nur die beiden direkt bei Wikipedia verlinkten Anleitungen unter http://www.nwlab.net/tutorials/wireshark/ (13.04.2010) und http://www.easy-network.de/ethereal.html (13.04.2010).

100 Siehe die Darstellung bei *Eckert*, IT-Sicherheit, S. 90 f. sowie *Brands*, IT-Sicherheitsmanagement, S. 37 ff.

Netzwerk erforderlich. Wie die Praxis des sog. `*Wardriving´*[101] zeigt, verfügen die WLAN-Router über enorme Funkreichweiten.[102] Ein Angreifer muss sich also nur in der Nähe aufhalten – was natürlich das Entdeckungsrisiko minimiert und den Kreis möglicher Angreifer maximal anwachsen lässt.

(3) Angriffe auf Router

Die Router selbst bergen durchaus ein Angriffspotential: Zum einen stehen die Router allein unter der Kontrolle ihres Betreibers. Dieser oder einer seiner Mitarbeiter kann Datenverkehr durch das Prinzip der temporären Zwischenspeicherung ohne Weiteres mitlesen.[103] Zum zweiten befinden sich Router teilweise auch in öffentlich zugänglichen Räumen, etwa in Universitäten.[104] Ein Mitlesen des IP-Verkehrs ist jedem möglich, der Zugang zu dem Gerät hat. Zuletzt sind Manipulationen der Routingprotokolle und Routingtabellen ohne Weiteres möglich (erfordern aber erhebliches technisches Know-how).[105] Datenpakete können so gezielt umgeleitet werden.[106]

(4) Angriffe auf Passwörter

Nutzer von Webmail-Diensten wie web.de, GMX oder Hotmail wählen häufig keine sicheren Passwörter, so dass diese leicht geknackt werden können.[107] Daneben sind alle Formen von Angriffen zur Erlangung von Passwörtern denkbar: Der Angreifer kann versuchen, das Passwort auszuspähen. Der Angreifer kann versuchen, das Passwort im Wege eines `*Social Engineering´*-Angriffs[108] genannt zu bekommen.

101 Darunter versteht man die systematische Suche nach WLANs, wobei in der Regel offene, das heißt nicht verschlüsselte WLANs gesucht werden, um kostenlos im Internet surfen zu können. Vgl. Wikipedia, Wardriving, Version vom 31.03.2009, 19.39 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Wardriving&oldid=58535758 sowie ausführlich zu technischer Vorgehensweise wie strafrechtlicher Bewertung *Bär,* MMR 2005, 434.

102 30 bis 100 Meter auf freier Fläche; Wikipedia, Wireless Local Area Network, Version vom 21.04.2009, 11.44 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Wireless_Local_Area_Network&oldid=592554 21.

103 *Vetter*, Gesetzeslücken bei der Internetkriminalität, S. 135 f.; *Holznagel*, Recht der IT-Sicherheit, S. 18; *Gassen*, Digitale Signaturen in der Praxis, S. 27.

104 *Schwenk*, Sicherheit und Kryptographie im Internet, S. 4.

105 Vgl. das Beispiel bei heise online vom 27.08.2008, "Router lügen nicht" - was, wenn doch?, verfügbar unter: http://www.heise.de/newsticker/Router-luegen-nicht-was-wenn-doch--/meldung/114984 (28.08.2008): „Dabei gibt es so gut wie keine Autorisierungsmechanismen, die Missbrauch verhindern könnten. Man verlässt sich im Wesentlichen darauf, dass das alles schon seine Richtigkeit hat."

106 *Schwenk*, Sicherheit und Kryptographie im Internet, S. 4.

107 Vgl. dazu etwa *Künnemann,* JurPC 62/2009, Rn. 15 ff.

108 Unter `*Social Engineering´* versteht man Angriffe, die nicht auf technischem Wege, sondern durch zwischenmenschliche Beeinflussung Informationen (wie Passwörter) oder Dienstleistungen zu erlangen versuchen; vgl. Wikipedia, Social Engineering, Version vom 01.12.2009,

Der Einsatz von `*Keyloggern*´, d.h. Hard- oder Software, die Tastatureingaben protokolliert,[109] ist möglich. Schließlich gibt es auch in diesem Bereich Fälle von Sicherheitslücken.[110]

(5) Angriffe auf von Dritten administrierte Systeme

Nutzer von Systemen, die sie nicht selbst und alleinig administrieren, sind weiteren Risiken ausgesetzt: Welcher Nutzer eines Internetcafés kann Aussagen über die Vertrauenswürdigkeit des Betreibers treffen (in dem Sinn, dass dieser seine Kunden nicht ausspäht und die Daten dann verkauft)? Welcher durchschnittliche Nutzer kann erkennen, ob der Betreiber eines Internetcafés über das erforderliche technische Know-how und die notwendige Zuverlässigkeit und Sorgfalt verfügt (so dass nicht wegen mangelhafter IT-Sicherheit das Risiko von Angriffen Dritter ansteigt)? Letztlich gelten derartige Bedenken gegenüber jedem Systemadministrator. Der Systemadministrator hat – technisch – etwa Zugriff zu auf dem Rechner vorhandenen E-Mail-Konten, persönlichen Daten, gespeicherten Passwörtern etc. Wer sein informationstechnisches System nicht vollständig selbst administriert, muss also darauf vertrauen, dass der Systemadministrator erstens seine technischen Befugnisse nicht missbräuchlich verwendet und zweitens alle erforderlichen Sicherheitsmaßnahmen trifft, damit auch außenstehenden Dritten ein Missbrauch nicht möglich ist.

(6) Zusammenfassung

Die Wege, vom Inhalt einer E-Mail Kenntnis zu nehmen, sind vielfältig. Welchen Weg ein Angreifer wählt, wird unter anderem von seiner speziellen Ausgangsposition (etwa Inhaberschaft bestimmter Zugriffsrechte zu bestimmten Netzwerken, als Administrator etc.), seinen technischen Kenntnissen,[111] seinen Ressourcen und seinen konkreten Interessen (geht es darum, ganz bestimmte Daten abzufangen oder geht es um die Sammlung möglichst vieler Daten gleichgültig von welchem Urhe-

17.01 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Social_Engineering&oldid=67491141; *Hartmann*, Sichere Kommunikation im Internet, S. 67.

109 Wikipedia, Keylogger, Version vom 01.02.2009, 20.41 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Keylogger&oldid=56127030.

110 Vgl. heise online vom 24.11.2008, Lücke in Google Mail ermöglicht Umleiten von Mails, verfügbar unter: http://www.heise.de/newsticker/Luecke-in-Google-Mail-ermoeglicht-Umleiten-von-Mails--/meldung/119348 (25.11.2008).

111 Wobei zu beobachten ist, dass die eigenen technischen Kenntnisse des Angreifers zunehmend an Bedeutung verlieren, da Entwicklung, Vertrieb und Support von Schadsoftware immer stärker zum Geschäftsmodell zu werden scheint. Heise online vom 10.06.2008, Trojanerbaukasten mit Rund-um-die-Uhr-Support und Austausch-Service, verfügbar unter: http://www.heise.de/newsticker/Trojanerbaukasten-mit-Rund-um-die-Uhr-Support-und-Austausch-Service--/meldung/109254 (11.06.2008) berichtet von einem Schadsoftware-Baukasten mit Funktionen wie Videostreaming über eine Webcam, Audiostreaming über Mikrofon usw. mit Online-Support (!) für 249 US-Dollar.

ber; wie wichtig ist dem Angreifer, dass sein Angriff unerkannt bleibt[112] etc.) abhängen. Die oben beschriebenen typischen Szenarien beziehen sich zwar zunächst auf den E-Mail-Dienst, gelten aber in weiten Teilen für sämtliche Kommunikationsinhalte: Der Möglichkeit des Abfangens und Mitlesens von Daten in LANs, WLANs und Routern sowie die stets bestehenden Zugriffsmöglichkeiten durch Systemadministratoren existieren hinsichtlich aller Arten von Kommunikationsdaten. Bedingt durch die technische Konzeption des „Netzwerks der Netzwerke", des Internets, gewährleistet es keinerlei Vertraulichkeit der darin übertragenen Kommunikationsdaten.

bb) Terminologie: Überwachen, Abhören, Ausspähen, Abfangen, Mitlesen

Eine einheitliche Terminologie für Angriffe auf die Vertraulichkeit von Daten in der digitalen Welt existiert bislang nicht. Häufig sind Begriffe wie überwachen, abhören, ausspähen, abfangen oder mitlesen zu finden. Die verwendeten Begriffe entstammen teilweise den parallelen „analogen" Zusammenhängen: So erinnert der Begriff des Abhörens an die Telekommunikationsüberwachung oder allgemein das Abhören des gesprochenen Worts (Lauschangriff); der Terminus „ausspähen" ist entsprechend an Spähangriffe angelehnt. Welcher Begriff im Einzelfall verwendet wird, hängt daher häufig vom konkreten Zusammenhang ab sowie davon, welche Aspekte eines Angriffs betont werden sollen. So rückt die Verwendung der Begriffe „mitlesen" oder „überwachen" die Kenntnisnahme durch Dritte in den Vordergrund, während das „Abfangen" von Daten zugleich auch die Möglichkeit der Datenunterdrückung oder Datenmanipulation (Angriffe auf die Integrität der Daten) impliziert.

Daher kann festgehalten werden, dass die verwendeten Termini keineswegs klar definiert und trennscharf gegeneinander abgrenzbar sind.[113] Eine präzisere (technische) Terminologie ist aber nicht ersichtlich. Insofern bleibt es auch im Rahmen dieser Arbeit bei der Übertragung analoger Begrifflichkeiten auf Vorgänge in der digitalen Welt. Trotz der damit einhergehenden mangelnden Definitions- und Abgrenzbarkeitsschärfe spricht für diese Vorgehensweise, dass die Verwendung hergebrachter analoger Terminologie ein intuitives Verständnis des Lesers für die technischen Vorgänge und damit insgesamt die Lesbarkeit fördert.

112 Dies wird für einen Angreifer etwa dann Priorität haben, wenn er an längerfristiger Überwachung interessiert ist oder wenn er im Falle seiner Entdeckung Strafverfolgung riskieren würde.

113 Dies spiegelt sich auch auf rechtlicher Ebene wieder; so finden sich allein im StGB Normen, die das Ausspähen (§ 202a StGB), Abfangen (§ 202b StGB), Löschen, Unterdrücken, Unbrauchbarmachen sowie Verändern (§ 303a StGB) von Daten unter Strafe stellen. Insbesondere die vier letztgenannten Begriffe können nicht genau abgegrenzt werden und überscheiden sich. Laut *Weidemann*, in: *v. Heintschel-Heinegg,* Beck OK StGB, § 303a, Rn. 7 sollte dadurch ein möglichst umfassender Schutz erreicht werden.

c. Technikbedingt fehlende Vertraulichkeit von Kommunikationsumständen (Anonymität) in der digitalen Welt

Im Hinblick auf die technische Funktionsweise von Datenübertragungen via Internet genießen nicht nur Kommunikationsinhalte, sondern auch Kommunikationsumstände keinerlei Vertraulichkeit:

aa) Technikbedingt fehlende Vertraulichkeit von E-Mail- und IP-Adresse

Für die E-Mail-Adresse und die zugehörige IP-Adresse des Empfängers einer E-Mail liegt dies auf der Hand: Diese werden ja gerade benötigt, um ihn als Empfänger der E-Mail zu identifizieren. Die Daten sind dazu bestimmt, nicht vertraulich zu sein. Jedem, der sich ins Internet einwählt, wird eine IP-Adresse zugewiesen, um seinen Rechner eindeutig zu identifizieren. *Die eindeutige Identifizierbarkeit ist nicht nur Voraussetzung zum Senden und Empfangen von E-Mails oder sonstiger Individualkommunikation. Alle Daten(pakete) – gleich welchen Inhalts – benötigen die IP-Adresse zur eindeutigen Bestimmung des Ziels eines Datenpakets.*[114] Das Aufrufen der allgemein zugänglichen Inhalte des `*World Wide Web*´ (WWW) erfordert ebenfalls, dass der Rechner des Nutzers, der die Inhalte betrachten will, eindeutig über die IP-Adresse identifizierbar ist – da ansonsten die Datenpakete nicht zu seinem Rechner geroutet werden können.

bb) Technikbedingt fehlende Vertraulichkeit des E-Mail-Headers

E-Mails enthalten neben ihrem Inhalt (der im sog. `*body*´ der E-Mail enthalten ist) und der E-Mail- sowie IP-Adresse des Empfängers im Kopfbereich (dem sog. `*header*´) der E-Mail weitere Informationen, nämlich die E-Mail-Adresse des Absenders sowie seine IP-Adresse, das Datum der Erstellung der E-Mail sowie alle Stationen, die die E-Mail auf ihrem Übertragungsweg passiert hat.[115] Diese Angaben sind nicht nur Sender und Empfänger bekannt, sondern – bedingt durch das System des Routing über mehrere Zwischenstationen – auch allen diesen Vermittlungsrechnern.

114 Siehe zur Adressierung und eindeutigen Identifizierbarkeit in Subnetzen oben FN 80.

115 Wikipedia, E-Mail, Version vom 01.12.2008, 13.46 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=E-Mail&oldid=53630851.

cc) Technikbedingte Zwischenspeicherung und Protokollierung von Kommunikationsumständen

Diese Informationen über Kommunikationsumstände fallen nicht nur in dem Moment an, in dem sie technisch benötigt werden, und werden dann verworfen, sondern werden grundsätzlich gespeichert:

Für E-Mails folgt dies bereits aus dem *`store-and-forward´*-Prinzip des Routing selbst, welches eine Zwischenspeicherung der E-Mail auf den einzelnen Routern, über die die E-Mail zu ihrem Ziel weitergeleitet wird, vorsieht.

Darüber hinaus protokollieren beispielweise E-Mail-Server[116] und Webserver[117] Aktionen und Fehlermeldungen. Diese werden in so genannten Logdateien (*`log files´*) gespeichert. Sie dienen vor allem der Fehleranalyse. Die Logdateien eines Webservers enthalten z.B. die Informationen, von welcher IP-Adresse zu welcher Uhrzeit welche konkreten Inhalte abgerufen wurden. Die Logdateien eines E-Mail-Servers protokollieren, unter welcher E-Mail-Adresse zu welcher Uhrzeit welcher E-Mail-Text an welche Empfänger-E-Mail-Adresse versendet wurde. Sowohl Kommunikationsinhalte als auch Kommunikationsumstände – sei es im Rahmen von Kommunikation oder sei es beim Surfen im Internet – werden protokolliert.

dd) Möglichkeit der individuellen Zuordnung von Kommunikationsverhalten

Über die E-Mail- oder IP-Adresse sind diese Informationen über Kommunikationsinhalte und -umstände auch konkreten Personen technisch zuordenbar (hier als technischer Personenbezug bezeichnet – in Abgrenzung zum datenschutzrechtlichen Begriff des Personenzugs bzw. der Personenbeziehbarkeit[118]):

116 Unter E-Mail-Server versteht man die Soft- bzw. Hardware, die E-Mails verwaltet, d.h. diese empfängt, sendet, speichert oder weiterleitet; Wikipedia, Mailserver, Version vom 23.07. 2008, 17.13 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Mailserver&oldid=48722289.

117 Webserver sind Computer, auf denen Webseiten und andere Internetinhalte gespeichert sind, und der diese Inhalte z.B. an Webbrowser überträgt; Wikipedia, Webserver, Version vom 13.04.2009, 15.27 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Webserver&oldid=58978426.

118 In einer datenschutzrechtlichen Perspektive ist nämlich umstritten, ob IP-Adressen Personenbezug aufweisen; vgl. zum Streitstand mit vielen weiteren Nachweisen *Meyerdierks,* MMR 2009, 8; *Brunst*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, S. 342 ff.; *Heidrich,* CR 2009, 168, 171 sowie jüngst VG Wiesbaden, Beschluss vom 27.02. 2009, Az.: 6 K 1045/08.WI, Rn. 38 f., das einen Personenbezug bejaht. Dabei besteht aber auch auf rechtlicher Ebene Einigkeit darüber, dass *technisch* immer ein Personenbezug hergestellt werden kann – nichts anderes wird hier behauptet. Die rechtliche Kontroverse ist der Tatsache geschuldet, dass nicht jeder Zugriff auf die Informationen hat, um den Personenbezug auch tatsächlich herstellen zu können (sog. Relativität des Personenbezugs). Unumstritten ist, dass technisch ein Personenbezug hergestellt werden kann.

Im Fall einer E-Mail-Adresse oder einer statischen IP-Adresse besteht dieser technische Personenbezug direkt ohne Zwischenschritte;[119] im Fall der Nutzung einer dynamischen IP-Adresse[120] kann der Personenbezug erst durch weitere Schritte hergestellt werden.[121] Die entsprechenden Logdateien des Internetproviders, der die IP-Adresse zugewiesen hat, müssen ausgewertet werden.[122] Dazu ist erforderlich, dass

- die Daten zum einen noch gespeichert sind (Rechtsgrundlagen hierfür können § 96 I Nr. 1, II TKG[123] i.V.m. §§ 97, 99, 100 oder 101 TKG[124] sein.[125])

119 Ohne Zwischenschritte meint hier, dass kein Rückgriff auf irgendwelche Logdateien erforderlich ist. Statische IP-Adressen gehören vielmehr – wie etwa eine Telefonnummer – zu den dauerhaft gespeicherten Bestandsdaten. Schließlich kann auch eine Privatperson direkt beim RIPE NCC registriert sein; *Heidrich,* CR 2009, 168, 171.

120 Hier wird dem Nutzer für jede Internetverbindung neu eine IP-Adresse von seinem Internetprovider zugewiesen. Dies ist der Regelfall.

121 Siehe zur Vorgehensweise *Brunst*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, S. 419 ff. Gleiches gilt, wenn eine IP-Adresse von mehreren Nutzern verwendet wird – sei es über eine Aufteilung der Ports, sei es über ein privates Subnetz (Vgl. FN 80). Fraglich ist allein, ob Daten, wem wann welche Ports unter welcher IP-Adresse oder welche lokale IP-Adresse unter welcher öffentlichen IP-Adresse zugewiesen waren, noch gespeichert sind. Angefallen und zumindest aus technischen Gründen für die Dauer einer Sitzung gespeichert worden sind diese Daten in jedem Fall. Für die technische Bejahung eines Personenbezugs reichts das aus. Ausführlich dazu Wikipedia, Network Address Translation, Version vom 12.03.2010, 12.10 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Network_Address_Translation&oldid=71685948.

122 Siehe dazu oben unter a. sowie ausführlich zur Protokollierung von IP-Adressen *Brunst*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, S. 346 ff.

123 § 96 TKG [Verkehrsdaten]: „(1) Der Diensteanbieter darf folgende Verkehrsdaten erheben und verwenden, soweit dies für die in diesem Abschnitt genannten Zwecke erforderlich ist: 1.die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten, […] (2) Die gespeicherten Verkehrsdaten dürfen über das Ende der Verbindung hinaus nur verwendet werden, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 genannten oder für die durch andere gesetzliche Vorschriften begründeten Zwecke erforderlich sind. Im Übrigen sind Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen. (…)“

124 Zum Zweck der Entgeltermittlung und Abrechnung (§ 97 TKG), zur Störungserkennung und –beseitigung sowie Missbrauchsbekämpfung (§ 100 TKG) und zur Auskunft über den Anschlussinhaber bei belästigenden oder bedrohenden Anrufen (§ 101 TKG; inwieweit die Norm auf IP-Adressen anwendbar ist, wäre noch genauer zu untersuchen). Das Verlangen des Kunden nach einem Einzelverbindungsnachweis (§ 99 TKG) rechtfertigt ebenfalls die Speicherung von Daten nach § 96 II TKG, spielt in diesem Zusammenhang aber keine Rolle.

125 § 109 I, II TKG stellen dagegen nach hier vertretener Auffassung keine Rechtsgrundlage für die Speicherung von Logdateien dar. § 109 TKG normiert lediglich die Verpflichtung von Diensteanbietern zu technischen Schutzmaßnahmen. Rechtsgrundlage für die Erhebung und Verwendung (so die Terminologie des TKG) von Daten zur Störungserkennung und Missbrauchsbekämpfung ist allein § 100 I TKG – wie sich aus seinem Wortlaut ergibt: „§ 100 TKG [Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten] (1) Soweit erforderlich, darf der Diensteanbieter zum Erkennen, Eingrenzen

- und zum anderen eine Rechtsgrundlage für diese Auskunft besteht und deren Voraussetzungen gegeben sind. In Betracht kommen etwa § 100g StPO und § 20m BKAG sowie verschiedene Landesverfassungsschutzgesetze[126] und Landespolizeigesetze,[127] aber auch richterliche Anordnungen zur Sicherung privatrechtlicher Ansprüche auf Auskunftserteilung (etwa § 101 IX UrhG).[128]

Anonyme, im Sinne von nicht zuordenbare Kommunikation und Information ist im Internet grundsätzlich nicht gewährleistet. Eine Speicherung zu Zwecken der Störungserkennung und Missbrauchsbekämpfung ist stets möglich und findet auch in der Breite statt.[129] Diese Daten können dann – bei Vorliegen der gesetzlichen Voraussetzungen - sowohl zu Zwecken der Strafverfolgung wie der Gefahrenabwehr und Gefahrenvorsorge verwendet werden.

ee) Möglichkeit der Generierung und Zuordnung individueller Nutzerprofile

Daneben können auch private Dritte Informations- und Kommunikationsverhalten auswerten (etwa durch Auswertung von Logdateien eigener Webserver, durch die Verwendung von `*Cookies*´[130], über den Dienst `*Google Analytics*´[131] sowie – vor

oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden. (…)". Soweit etwa *Bock*, in: *Geppert/Piepenbrock/Schütz/Schuster,* Beck TKG-Komm, § 109, Rn. 19 vertritt, § 109 rechtfertige „die Überwachung des eigenen Netzes mittels Intrusion-Detection-System auf verdächtige Muster (Signaturen) im IP-Verkehr, die auf einen Hacker-Angriff aus dem äußeren Netz oder innerhalb des eigenen Netzes hindeuten", dürfte sich dies allenfalls auf eine Echtzeitüberwachung und –filterung des IP-Verkehrs, aber nicht auf eine Speicherung von Daten beziehen. Dafür existiert mit § 100 I TKG bereits eine Rechtsgrundlage. Das BVerfG scheint diese Sichtweise zu teilen, vgl. BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 6. Vor dem Urteil des BVerfG vom 02.03.2010, Az.: 1 BvR 256/08 et al., mit dem die Regelungen zur Vorratsdatenspeicherung in den §§ 113a, b TKG für nichtig erklärt wurden, wären diese ebenfalls als Rechtsgrundlage in Frage gekommen.

126 Z.B. § 24a II S. 1, Nr. 4 Landesverfassungsschutzgesetz Mecklenburg-Vorpommern, § 5a VI Niedersächsisches Verfassungsschutzgesetz, Art. 6c II S. 1 Nr. 4 Bayerisches Verfassungsschutzgesetz.

127 Z.B. § 34a I Nr. 1 thüringisches Polizeiaufgabengesetz, § 34b II S. 1, Nr. 1, III Bayerisches Polizeiaufgabengesetz, § 23a I baden-württembergisches Polizeigesetz.

128 Vgl. dazu etwa jüngst OLG Karlsruhe, Beschluss vom 01.09.2009, Az.: 6 W 47/09, verfügbar unter http://lrbw.juris.de/cgi-bin/laender_rechtsprechung/document.py?Gericht=bw&GerichtAuswahl=OLG+Karlsruhe&Art=en&Datum=2009&nr=11936&pos=1&anz=40 (23.09.2009).

129 Insbesondere bei Web- und E-Mail-Servern wird Datenverkehr standardmäßig mitgelogt; vgl. dazu Wikipedia, Logdatei, Version vom 08.02.2010, 17.59 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Logdatei&oldid=70410650, sowie Wikipedia, Logdateianalyse, Version vom 23.03.2010, 14.59 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Logdateianalyse&oldid=72262886.

130 Die hier vor allem angesprochenen HTTP-Cookies sind Dateien auf dem Rechner des Nutzers, in denen nutzerbezogene Informationen gespeichert werden (etwa sitzungsübergreifend persönliche Einstellungen oder innerhalb einer Sitzung alle in den Warenkorb gelegten Artikel); Wikipedia, HTTP-Cookie, Version vom 11.04. 2009, 10.38 Uhr, verfügbar unter: http://

allem bei Internet Service Providern - `*Deep Packet Inspection´*[132]).[133] Sog. `*tracking cookies´* können auch den Besuch verschiedener Webseiten innerhalb einer Internetsitzung durch den Nutzer mitverfolgen. Dadurch können verschiedene Informationen miteinander verknüpft werden, etwa das Surfverhalten des Nutzers mit einem konkreten Nutzerprofil bei einem Online-Shop.[134] Die Möglichkeit der Generierung umfassender Nutzerprofile kann aber durch die nutzerseitig restriktive Handhabung der Zulassung von `*Cookies´* und/oder deren regelmäßige Löschung reduziert wer-

de.wikipedia.org/w/index.php?title=HTTP-Cookie&oldid=58906659. Dazu auch ausführlich *Brands*, IT-Sicherheitsmanagement, S. 191 f. sowie *Brunst*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, S. 58 ff. Eine rechtliche Bewertung der Nutzung von Cookies vgl. bei Hoeren, Skript Internetrecht (Stand Feb. 2010), verfügbar unter: http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Internetrecht_Februar2010.pdf (30.03.2010), S. 395 ff.

131 Der Bundesdatenschutzbeauftragte *Schaar* hält lt. heise online vom 20.11.2009, Bundesdatenschutzbeauftragter kritisiert Usertracking bei Krankenkassen, verfügbar unter: http://www.heise.de/newsticker/meldung/Bundesdatenschutzbeaftragter-kritisiert-Usertracking-bei-Krankenkassen-864903.html (23.11.2009) die Nutzung von `*Google Analytics´* für datenschutzrechtlich „unzulässig, da die derzeitige Konfiguration des Dienstes eine wirksame Wahrnehmung des Rechts auf Widerspruch, Information und Auskunft sowie Löschung der Daten durch den Betroffenen nicht ermöglicht". Zu weiteren datenschutzrechtlichen Bedenken siehe Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Datenschutzrechtliche Bewertung des Einsatzes von Google Analytics, verfügbar unter: https://www.datenschutzzentrum.de/tracking/20090123_GA_stellungnahme.pdf (02.07. 2009).

132 Dabei werden die Datenpakete in einem Netzwerk nicht nur hinsichtlich ihres `*Headers´*, sondern auch inhaltlich untersucht. Diese Filterung dient einerseits dem Schutz vor Protokollverletzungen, Viren, Spam etc. und damit sinnvollen und legitimen Zielen; Wikipedia, Deep Packet Inspection, Version vom 28.05.2009, 12.17 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Deep_Packet_Inspection&oldid=60516024. In den USA und in Großbritannien werten Internet Service Provider mittels `*Deep Packet Inspection´* aber auch umfassend Surfverhalten, E-Mails, Peer-to-Peer-Tauschaktionen usw. aus (soweit der Datenverkehr nicht verschlüsselt ist) und verkaufen diese Nutzerprofile an Werbeanbieter für sog. `*behavioral advertisement´*; *Spies,* MMR 2008, XII, XII f. Die Europäische Kommission sieht wegen des Fehlens einer Einwilligung der Nutzer europäisches Datenschutzrecht verletzt und hat ein Vertragsverletzungsverfahren gegen Großbritannien eingeleitet; Europäische Kommission, Pressemitteilung vom 14.04.2009, verfügbar unter: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570&format=HTML&aged=0&language=DE&guiLanguage=en (03.06.2009).

133 Vergleiche allgemein zur den Verknüpfungsmöglichkeiten von digitalen Identitäten Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Verkettung digitaler Identitäten, verfügbar unter: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf (05.11.2007), wobei sich die Darstellung auf datenschutzrechtlich zulässige Maßnahmen beschränkt (während in Wirklichkeit häufig nicht-datenschutzkonformes Verhalten festgestellt werden muss). Einen Überblick über Identifizierungsmöglichkeiten und Optionen der Profilbildung bietet *Brunst*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, S. 74 ff, 32 ff.

134 Siehe eine Darstellung der Verknüpfungsmöglichkeiten sowie eine umfassende Darstellung der datenschutzrechtlichen Bewertung bei *Ihde,* CR 2000, 413.

den.[135] Bestimmte Programme können auch die Browser-History[136] von Nutzern auslesen und so an ein sitzungsübergreifendes Nutzerprofil kommen.[137] Schutzmaßnahmen des Nutzers können etwa durch ein Löschen der Browser-History am Ende jeder Sitzung erfolgen - dadurch büßt er aber zugleich auch die Bequemlichkeit dieser Funktion ein.[138]

Die großen Suchmaschinenbetreiber, allen voran Google, aber auch Yahoo, verfügen über riesige Mengen an auswertbaren Nutzerdaten sowie ausgefeilte Techniken des Data Mining.[139] Google verwendet darüber hinaus `*tracking cookies*´ zur Verfolgung des Surfverhaltens des Nutzers über verschiedene Seiten hinweg.[140] Dadurch können unter Umständen individuelle Nutzerprofile konkreten Personen zugeordnet werden.

Die Vertraulichkeit von Informations- und Kommunikationsverhalten im Internet kann mithin nicht nur in bestimmten Fällen zur Strafverfolgung oder Gefahrenabwehr aufgehoben werden, sondern ist dauerhaft und in nicht vom Nutzer durch sein (gesetzeskonformes) Verhalten beeinflussbarer Weise durch private Dritte bedroht. Weder die Umstände noch die Inhalte von Informations- und Kommunikationsverhalten genießen somit in einer technischen Betrachtung im Internet Vertraulichkeit. Jeder Interessierte kann Kommunikation mitlesen und Informationsverhalten nachvollziehen.

2. Gestiegene Notwendigkeit der Gewährleistung von Vertraulichkeit in der digitalen Welt

Gleichzeitig ist der Bedarf an Vertraulichkeit exponentiell angestiegen:

135 Einzelheiten siehe unter Wikipedia, HTTP-Cookie, Version vom 11.04.2009, 10.38 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=HTTP-Cookie&oldid=58906659.

136 Das Verlaufsprotokoll des Browsers, in dem alle aufgerufenen Internetseiten gespeichert werden.

137 Siehe heise Security vom 02.03.2007, Angreifer können Liste besuchter Webseiten auslesen, verfügbar unter: http://www.heise.de/security/Angreifer-koennen-Liste-besuchter-Webseiten-auslesen--/news/meldung/86113 (28.04.2009).

138 Zu weiteren Möglichkeiten, das Informations- und Kommunikationsverhalten zu beobachten und auszuwerten, vgl. Köhntopp/Köhntopp, Datenspuren im Internet, verfügbar unter: http://kris.koehntopp.de/artikel/daten spuren/CR_Datenspuren_im_Internet.pdf (05.05.2009), S. 8 ff.

139 Vgl. umfassend zu Techniken des Data Mining Wikipedia, Data Mining, Version vom 16.03.2009, 21.54 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Data_Mining&oldid=57972338.

140 heise online vom 12.08.2008, US-Repräsentantenhaus erwärmt sich für Online-Datenschutzgesetz, verfügbar unter: http://www.heise.de/newsticker/US-Repraesentantenhaus –erwaermt-sich-fuer-Online-Datenschutzgesetz--/meldung/114144 (13.08.2008).

a. Internetnutzung als gesellschaftliches Massenphänomen

Die Nutzung des Internets für Information und Kommunikation ist zum alltäglichen Massenphänomen geworden, vor allem in den Industriestaaten:[141]

- In Deutschland nutzen 73 Prozent der erwachsenen Bevölkerung das Internet.[142]
- Briefliche und teilweise auch telefonische Kommunikation werden zunehmend abgelöst durch die Kommunikation per E-Mail. 88 Prozent der deutschen Internetnutzer kommunizieren per E-Mail.[143]
- Führendes Nachrichtenmedium bleibt zwar das Fernsehen, das Internet gewinnt aber zunehmend an Bedeutung, vor allem hinsichtlich multimedialer Angebote wie Online-Videos und Fernseh- oder Radio-Streams.[144]

b. Keine hergebrachter Mediennutzung und Kommunikationswege entsprechende Vertraulichkeitsgewährleistung

Dies führt zu einem gewandelten Vertraulichkeitsbedarf von Informations- und Kommunikationsverhalten. Die Vertraulichkeitskonzepte hergebrachter Mediennutzung und Kommunikationswege existieren nicht in vergleichbarer Weise bei internetbasierter Information und Kommunikation:

- Während der Zugriff auf einen Brief oder das Abhören eines Telefonats zu irgendeinem Zeitpunkt einen realen, körperlichen Zugriff (auf den Brief im Briefkasten oder im Briefverteilzentrum, auf das Telekommunikationsendgerät eines Beteiligten oder die Leitung vom Endgerät bis zum nächsten Schaltkasten) erfordert,[145] können E-Mails allein durch Maßnahmen in der digitalen Welt abge-

141 Diese Veränderungen können weltweit festgestellt werden; allerdings sind sie in Entwicklungsländern zumeist weniger stark ausgeprägt (vgl. zur weltweiten Internetnutzung heise online vom 06.10.2007, Digitale Kluft verfestigt sich laut weltweiter Umfrage, verfügbar unter: http://www.heise.de/newsticker/Digitale-Kluft-verfestigt-sich-laut-weltweiter-Umfrage--/meldung/97000 (07.04.2009)). Hier liegt der Fokus der Betrachtung auf der Situation in Deutschland bzw. Westeuropa.

142 Statistisches Bundesamt Deutschland, Pressemitteilung vom 03.12.2009, verfügbar unter: http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Presse/pm/2009/12/PD09__464__IKT,templateId=renderPrint.psml (08.12.2009).

143 Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2009, verfügbar unter: http://www.bsi.bund.de/literat/lagebericht/Lagebericht2009.pdf (09.03.2009), S. 12.

144 heise online vom 10.06.2008, Zahl deutscher Internet-Nutzer wächst um fünf Prozent, verfügbar unter: http://www.heise.de/newsticker/Zahl-deutscher-Internet-Nutzer-waechst-um-fuenf-Prozent--/meldung/109249 (11.06.2008).

145 Das macht einen solchen Zugriff schwieriger realisierbar und wegen der notwendigen körperlichen Anwesenheit zu Manipulationszwecken steigt das Entdeckungsrisiko. Insofern geht es nicht primär darum, ob ein Abhören von Telefonleitungen technisch leicht möglich ist (etwa durch Anklemmen eines weiteren Apparats am Schaltkasten), sondern es geht darum, ob ein *unentdecktes* Abhören leicht ist; *Schwenk*, Sicherheit und Kryptographie im Internet, S. 4.

fangen und mitgelesen werden. Daher müssen (technische) Maßnahmen getroffen werden, um die Vertraulichkeit von Kommunikations*inhalten* bei Internetkommunikation wie bei hergebrachter telefonischer oder brieflicher Kommunikation abzubilden.

- Zum anderen ist ein neues Konzept erforderlich, um Anonymität, also Vertraulichkeit von Informations- und Kommunikations*umständen* zu gewährleisten: Hergebrachte Radio- und Fernsehnutzung sind vollkommen anonym; niemand kann nachvollziehen, wer wann welche Sendung angesehen hat oder nicht. Auch Printmedien können anonym erworben werden und in jedem Fall bleibt vertraulich, für welche Inhalte sich der Leser im Einzelnen interessiert.

c. Zunahme der Vertraulichkeitsgefahren

Zugleich sind Daten über Informations- und Kommunikationsverhalten Gefährdungsszenarien von völlig neuer Qualität und Quantität ausgesetzt. Während die Nutzung von Kommunikationsinfrastrukturen wie dem Internet zunehmend alltäglich wird, sind mit der digitalen Kommunikationstechnik neue Angriffsflächen entstanden und hat ein Überwachen, Ausspähen und Auswerten[146] von Daten ungeahnte Verwendungsmöglichkeiten und (finanzielle) Attraktivität erhalten. Diese Gefährdungslage besitzt keine Ähnlichkeit mehr mit der früheren Gefahr, dass der Nachbar oder ein Postmitarbeiter Telefonate abhört. Darüber hinaus sind folgende Faktoren zu berücksichtigen, die ebenfalls zu einer substantiellen Veränderung der Gefährdungslage beitragen: die Möglichkeit der spurenlosen Überwachung,[147] die Möglichkeit der Sichtung großer Datenmengen durch Filterverfahren[148] und die Multiplikation der durch nicht-staatliche Akteure drohenden Gefahren.[149]

Zusammenfassend kann dies auf die Formel gebracht werden: *Dem Verschwinden von Vertraulichkeit des Informations- und Kommunikationsverhaltens des Einzelnen steht ein wachsendes Bedürfnis nach der Gewährleistung von Vertraulichkeit gegenüber.*

Dies verkennt *Lindloff*, E-Mail-Kommunikation von Rechtsanwälten mit Mandanten und Gerichten, S. 96.

146 Vgl. zur Terminologie oben unter b.bb.

147 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 182.

148 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 183.

149 Nach *Schwenk*, Sicherheit und Kryptographie im Internet, S.5 sind nahezu alle Rechner, die längere Zeit im Internet sichtbar sind, von so genannten „Port Scans" betroffen, die meist der Vorbereitung von Angriffen dienen.

3. Verschlüsselung zur Gewährleistung der Vertraulichkeit von Kommunikationsinhalten

Die erforderliche Gewährleistung der Vertraulichkeit von Inhalt und Umständen von Informations- und Kommunikationsverhalten im Internet wird technisch durch Verschlüsselungsverfahren umgesetzt: Verschlüsselungsverfahren wurden gerade zum Zweck der Gewährleistung von inhaltlich vertraulicher Kommunikation entwickelt. Verwendet werden können sowohl symmetrische wie auch asymmetrische Verfahren. Für die Kommunikation per E-Mail werden vor allem asymmetrische Verfahren eingesetzt, da diese keinen vorherigen Schlüsselaustausch über einen sicheren Kommunikationskanal erfordern. Der öffentliche Schlüssel eines Nutzer ist vielmehr entweder ohnehin im Internet veröffentlicht oder kann ungefährdet per unverschlüsselter E-Mail übersandt werden.

a. Steganographie als alternatives Verfahren der Vertraulichkeitssicherung?

Steganographische Verfahren dienen ebenfalls dazu, Botschaften im Geheimen zu übermitteln, allerdings nicht durch Chiffrieren, sondern durch Verstecken der Nachricht.[150] Bei Verschlüsselungsverfahren wird nicht geheim gehalten, dass eine Nachricht übermittelt wird, es soll Dritten nur unmöglich sein, den Inhalt der Nachricht zur Kenntnis zu nehmen. Bei steganographischen Verfahren ist es umgekehrt: Es wird geheim gehalten, dass überhaupt eine Nachricht übermittelt wird und auf diese Weise soll eine - grundsätzlich mögliche - Kenntnisnahme verhindert werden.[151]

> „Steganographie der Moderne definiert sich folgendermaßen: Eine geheimzuhaltende Nachricht wird in eine Hülle derart eingebettet, dass dem Ergebnis erstens die minimalen Veränderungen kaum bzw. nicht anzusehen sind und zweitens die Veränderungen nicht mit Methoden nachweisbar sind.“[152]

Während ein frühes steganographisches Verfahren etwa das Schreiben mit unsichtbarer Tinte war,[153] wird heute nicht mehr Papier zum Verstecken von Nachrichten verwendet, sondern in der Regel Bilddateien. Da die meisten Graphikstandards mehr Farbabstufungen bieten als der Mensch wahrnehmen kann[154] und alle Bilddateien ohnehin über ein gewisses unvermeidbares so genanntes „Hintergrundrau-

150 Das Wort ‚Steganographie‘ stammt ebenfalls aus dem Griechischen und bedeutet ‚verdecktes Schreiben‘; *Federrath*, Steganographie - vertrauliche Kommunikation ohne Kryptographie, in: *Hamm/Möller,* Datenschutz durch Kryptographie, S. 42, 42.

151 Vgl. dazu ausführlich Wikipedia, Steganographie, Version vom 22.04.2009, 10.47 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Steganographie&oldid=59289188.

152 *Federrath*, Steganographie - vertrauliche Kommunikation ohne Kryptographie, in: *Hamm/Möller,* Datenschutz durch Kryptographie, S. 42, 42.

153 *Schneier*, Angewandte Kryptographie, S. 11.

154 *Schneier*, Angewandte Kryptographie, S. 11.

schen“[155] verfügen, können Nachrichten dort sehr leicht versteckt werden.[156] Häufig wird man eine Kombination von Verschlüsselungs- und steganographischen Verfahren antreffen können: Die Nachricht wird nicht nur verschlüsselt, so dass niemand sie inhaltlich zur Kenntnis nehmen kann, sondern zusätzlich wird auch die bloße Existenz einer Nachricht verborgen.

Steganographische Verfahren können aber nach dem derzeitigen Stand der Technik nicht als Alternative zu Verschlüsselungsverfahren hinsichtlich der Gewährleistung von Vertraulichkeit qualifiziert werden:[157] Symmetrische steganographische Verfahren[158] sind zwar grundsätzlich geeignet, Vertraulichkeit zu gewährleisten. Sie weisen aber erstens dasselbe Defizit auf wie die symmetrischen Verschlüsselungsverfahren: die Erforderlichkeit eines vorherigen Schlüsseltausches über einen sicheren Kanal. Schließlich wäre zweitens noch zu diskutieren, ob tatsächlich ein vergleichbares Sicherheitsniveau durch ein Verstecken der Kommunikation erreicht wird.[159] Die Sicherheit von steganographischen Verfahren scheint aber noch nicht ansatzweise so intensiv untersucht worden zu sein wie dies für Verschlüsselungsverfahren geschehen ist. Bedeutsamer sind angesichts weltweiter Massenkommunikation via E-Mail ohnehin die asymmetrischen Verfahren, bei denen der öffentliche Schlüssel frei verfügbar ist. Solche Verfahren gibt es zwar auch in der Steganographie, diese existieren aber bislang eher theoretisch als in der praktischen Anwendung und sind schwer realisierbar.[160]

Steganographische Verfahren könnten somit theoretisch eine Alternative zu Verschlüsselungsverfahren für die Gewährleistung von Vertraulichkeit darstellen – sind dies nach dem Stand der Technik aber (noch?) nicht.

155 Der Begriff des (Hintergrund- oder Daten-)Rauschens bezieht sich auf die natürlich vorhandenen Variationen in Daten; vgl. Wikipedia, Steganographie, Version vom 22.04.2009, 10.47 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Steganographie&oldid=59289188; *Koch,* CR 1997, 106, 107. Insbesondere Bilddatei- sowie Tondaten sind für Steganographie geeignet, da sie eine vergleichsweise hohe Redundanz aufweisen.

156 Vgl. auch die Darstellung der Funktionsweise von Steganographie bei *Koops*, The crypto controversy, S. 46 f.

157 *Schneier*, Secrets and Lies, S. 245 f. weist außerdem darauf hin, dass eine mit dem Verstecken von Nachrichten in Bild- oder Musikdateien einhergehende Abweichung von vorherigen Kommunikationsmustern (die Kommunikationspartner haben sich zuvor nie Bilder geschickt etc.) den Effekt des „versteckten“ Nachrichtenaustauschs zunichtemachen kann, da das Kommunikationsverhalten jedem abhörenden Geheimdienst verdächtig vorkäme.

158 Auch bei steganographischen Verfahren werden symmetrische und asymmetrische Verfahren unterschieden.

159 *Roßnagel/Pfitzmann*, Datenschutz im Internet, in: *Staudt,* Deutschland online, S. 89, 91 sprechen vorsichtig davon, dass gute steganographische Verfahren nicht oder nur schwer zu enttarnen seien.

160 Wikipedia, Steganographie, Version vom 22.04.2009, 10.47 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Steganographie&oldid=59289188.

b. Sonstige alternative Verfahren der Vertraulichkeitssicherung?

Nach dem derzeitigen Stand der Technik existieren keine alternativen Verfahren zur Gewährleistung der Vertraulichkeit von Kommunikation. Andererseits muss daran erinnert werden, dass Verschlüsselungsverfahren grundsätzlich nur *eine* Option zur Gewährleistung von IT-Sicherheit darstellen. Es mag sich um die beste Option oder um die am besten bekannte Option handeln, es handelt sich aber immer nur um *eine* technische Möglichkeit:

> "Cryptography is not the only means of providing information security, but rather one set of techniques."[161]

Sollte es in Zukunft andere Technologien geben, die Vertraulichkeit in vergleichbarer Weise wie Verschlüsselungsverfahren gewährleisten, dürften die rechtlichen Fragestellungen sowie die im Rahmen dieser Arbeit vorgestellten Antworten – soweit dies heute abzusehen ist – allerdings übertragbar sein:

- Jede Technologie, die Vertraulichkeit gewährleisten soll, muss ein so hohes Sicherheitsniveau verwirklichen, dass sie auch gegenüber äußerst ressourcenstarken Angreifern (wie etwa ausländischen Geheimdiensten) Sicherheit bietet - andernfalls wäre der Vertraulichkeitsschutz nicht effektiv.
- Ist der gewährleistete Vertraulichkeitsschutz effektiv, so ist er es grundsätzlich gegenüber jedem denkbaren „Angreifer" – auch wenn manche „Angriffe", etwa solche durch staatliche Sicherheitsbehörden, als legitim und legal anzusehen sind.
- Wird eine Zugriffsmöglichkeit für die staatlichen Sicherheitsbehörden offen gehalten, kann eine solche Zugriffsmöglichkeit prinzipiell (wie auch immer diese konkret ausgestaltet sein mag) von anderen Angreifern missbraucht werden.

Alternative Verfahren zur Gewährleistung der Kommunikationsvertraulichkeit wären folglich nur dann wesentlich anders zu beurteilen, wenn sie einerseits Vertraulichkeitsbeeinträchtigungen durch unerwünschte Angreifer effektiv verhindern, andererseits Vertraulichkeitsbeeinträchtigungen durch legitimierte „Angreifer" wie Sicherheitsbehörden aber umgekehrt ermöglichen.

Dies kann nach dem derzeitigen (und derzeitig absehbaren)[162] Stand der Technik allerdings nur auf eine Weise umgesetzt werden: durch einen *Informationsvorsprung* derjenigen, denen der Zugriff auf Kommunikation gewährt werden soll. Dieser Informationsvorsprung kann konkret im Wissen um eine Hintertür oder Sicherheitslücke des Verfahrens bestehen oder in (hinterlegten) Zusatzinformationen, mit deren Hilfe ein Kommunikationszugriff erfolgen kann. Entscheidend für die Realisierung der genannten Anforderungen ist die *Wahrung* dieses Informationsvorsprungs: Es muss effektiv verhindert werden, dass die Zusatzinformationen, die die Vertraulich-

161 *Menezes/van Oorschot/Vanstone*, Handbook of applied cryptography, S. 4.

162 Die Bearbeiterin mag hier technisch wenig visionär sein, doch geht es hier vor allem um auch in der Praxis realisierbare Modelle. Unter dieser Prämisse ist derzeit keine andere Umsetzung denkbar.

keit von Kommunikation aufzuheben imstande sind, nicht-legitimierten Personen bekannt werden.

Zusammenfassend kann festgehalten werden: Es gibt nach dem derzeitigen Stand der Technik keine alternativen Verfahren zur Gewährleistung der Kommunikationsvertraulichkeit. Sollten in Zukunft andere Verfahren als Verschlüsselungsverfahren existieren, die Kommunikationsvertraulichkeit zu gewährleisten im Stande sind, wären die rechtlichen Bewertungen übertragbar. Dies gilt so lange bis ein Verfahren das Dilemma zwischen Verhinderung illegitimer Kenntnisnahme einerseits und Ermöglichung staatlich legitimierter Kenntnisnahme andererseits lösen kann – ohne auf die Notwendigkeit der (technisch schwerlich realisierbaren) Wahrung eines Informationsvorsprungs angewiesen zu sein.

c. Vertraulichkeitsniveau: Leitungs- oder Ende-zu-Ende-Verschlüsselung?

Auch bei Verwendung von (sicheren) Verschlüsselungsverfahren können verschiedene Vertraulichkeitsniveaus unterschieden werden – je nachdem, zu welchem Zeitpunkt im Kommunikationsvorgang die Ver- bzw. Entschlüsselung erfolgt:[163]

- Bei der Leitungs- oder `*Link-by-Link*´-Verschlüsselung werden alle Daten zwischen zwei physikalischen Endpunkten (etwa zwei Routern) verschlüsselt. Dort werden die Daten entschlüsselt und für die Weitersendung an den nächsten physikalischen Endpunkt (einen weiteren Router oder den Zielrechner) erneut verschlüsselt.
- Bei der Ende-zu-Ende- oder englisch `*End-to-End*´-Verschlüsselung werden die Daten auf dem informationstechnischen System des Absenders verschlüsselt und erst ganz am Ende des Kommunikationsvorgangs auf dem Rechner des Empfängers wieder entschlüsselt.[164]

Zur Gewährleistung der Vertraulichkeit von Kommunikationsinhalten ist daher offensichtlich stets eine Ende-zu-Ende-Verschlüsselung erforderlich.[165] Diese umfasst – im Gegensatz zur Leitungsverschlüsselung – aber nicht die Kommunikati-

163 Bzw. auf welcher Ebene des ISO/OSI-Schichtenmodells eine Verschlüsselung erfolgt; siehe dazu ausführlich *Hartmann*, Sichere Kommunikation im Internet, S. 115 ff. sowie *Schneier*, Angewandte Kryptographie, S. 255 ff.

164 So auch die Definition von Ende-zu-Ende-Verschlüsselung gem. RFC 4949: Internet Security Glossary, Version 2 vom August 2007, verfügbar unter: http://www.heise.de/netze/rfc/rfcs/rfc4949.shtml (11.08.2009), S. 120: "[end-to-end encryption] (I) Continuous protection of data that flows between two points in a network, effected by encrypting data when it leaves its source, keeping it encrypted while it passes through any intermediate computers (such as routers), and decrypting it only when it arrives at the intended final destination. (…)".

165 So auch *Bizer,* KritJ 1995, 450, 461 sowie für Kommunikation über öffentliche Netze auch Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe zum Einsatz kryptografischer Verfahren, verfügbar unter: http://www.lda.brandenburg.de/media/2473/kryptoverfahren.pdf (21.04.2008), S. 19.

onsumstände. Hierzu ist zusätzlich eine Leitungsverschlüsselung bzw. der Einsatz anderer Anonymisierungstechniken erforderlich.[166]

4. Verschlüsselung zur Gewährleistung der Vertraulichkeit von Kommunikationsumständen (Anonymität)

Auch die Vertraulichkeit der Umstände von Informations- und Kommunikationsverhalten wird mit Hilfe von Verschlüsselungsverfahren gewährleistet. Technisch kann nicht auf die eindeutige Identifizierbarkeit des Rechners verzichtet werden, da nur anhand der IP-Adresse die Datenpakete an den Empfänger weitergeleitet werden können.

a. Einfache Anonymisierungstechniken

Die einfachste Methode zur Gewährleistung der Vertraulichkeit von Kommunikationsumständen ist daher, die individuelle Identifizierbarkeit zu beseitigen, indem man sich hinter einem anderen Rechner verbirgt. Dazu bieten sich vor allem sog. anonymisierende Proxyserver an.[167] Proxyserver[168] wirken als Vermittler, die Datenpakete, die versendet werden sollen, unter ihrer eigenen IP-Adresse weiterleiten

166 So auch Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, M 4.90 Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells, verfügbar unter: http://www.bsi.bund.de/gshb/deutsch/m/m04090.htm (07.01.2009). Zur Kombination von Ende-zu-Ende- und Leitungsverschlüsselung *Schneier*, Angewandte Kryptographie, S. 259 f.; zu anderen Anonymisierungstechniken sogleich.

167 Siehe dazu Wikipedia, Anonymität im Internet, Version vom 28.04.2009, 11.54 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Anonymit%C3%A4t_im_Internet&oldid=59491766; *Pfitzmann/Steinbrecher*, Digitale Glaubwürdigkeit und Privatsphäre in einer vernetzten Gesellschaft, in: *Klumpp/Kubicek/Roßnagel,* Next generation information society?, S. 290, 293 f. Beim anonymen Versand von E-Mails wird allerdings eher der Terminus `*Remailer´* verwendet; vgl. Wikipedia, Remailer, Version vom 18.08.2008, 12.38 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Remailer&oldid=49683822. Im Kern stimmen aber Vorgehensweise (Entfernen der Kopfdaten, des sog. `*Headers´*), einzuhaltende Grundsätze zur Gewährleistung effektiven Vertraulichkeitsschutzes sowie die zu diesem Zweck eingesetzten Maßnahmen überein. Vgl. insoweit nur Wikipedia, Cypherpunk Remailer, Version vom 29.12.2008, 01.05 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Cypherpunk_Remailer&oldid=54653538 sowie Wikipedia, Mixmaster-Remailer, Version vom 18.04.2009, 20.02 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Mixmaster-Remailer&oldid=59164566. Einen Überblick gibt *Brunst*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, S. 88 ff.

168 Lt. Wikipedia, Proxy (Rechnernetz), Version vom 04.04.2009, 20.22 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Proxy_(Rechnernetz)&oldid=58680295 von engl. `proxy representative´ - Stellvertreter bzw. lat. `proximus´ - der Nächste.

und eingehende Datenpakete an den Empfänger weiterreichen.[169] Um als Anonymisierungsdienst einsetzbar zu sein, darf der Proxy allerdings nicht – wie ansonsten üblich – über die Kopfdaten der Datenpakete erkennbar machen, dass es sich um einen Proxyserver handelt und von welchem dahinter stehenden Rechner oder Dienst (`*Client´*) die Daten stammen.[170] Denn allein aus dieser Veränderung der Kopfdaten resultiert die Nicht-Identifizierbarkeit des Absenders einer E-Mail durch den Empfänger der E-Mail ebenso wie die Nicht-Identifizierbarkeit eines Nutzers, der eine bestimmte Internetseite aufruft, durch den Provider, bei dem die Seite gehostet wird, und vor allem die Nicht-Identifizierbarkeit von Nutzern durch Dritte. Gründe für den Einsatz von Proxies gibt es allerdings viele und die Gewährleistung von (einer gewissen) Anonymität ist eher ein Nebeneffekt denn ein Ziel der Verwendung von Proxies.

Die alleinige Zwischenschaltung von Proxys gewährleitet aber keine verlässliche Anonymität. Zum einen kann natürlich der Proxy selbst über seine Log-Dateien im Nachhinein wieder zuordnen, wer wem eine E-Mail geschrieben hat und wer welche Internetseiten aufgerufen hat. Jenseits der Frage der Vertrauenswürdigkeit und technischen Verlässlichkeit des Proxies, kann Informations- und Kommunikationsverhalten jedoch auch durch Filterung des bei dem Proxy ein- und ausgehenden Datenverkehrs überwacht werden. Interessierten Dritten ist ein Mitlesen des Netzwerksverkehrs häufig möglich – ohne dass der einzelne Nutzer absehen kann, ob die von ihm genutzten Kommunikationswege diesbezüglich sicher und vertrauenswürdig sind oder nicht.

Die Benutzung nur *eines* Proxies als anonymisierenden Vermittlungsrechner kann daher keine wirkliche Anonymität bieten: Jedenfalls der Proxybetreiber selbst (oder ein erfolgreicher Angreifer auf den Proxy) können den Datenverkehr wiederum IP-Adressen zuordnen. Dritte können den Netzwerkverkehr abhören und so die entsprechende Zuordnung vornehmen. Anonymisierende Proxies gewährleisten daher keine Vertraulichkeit von Kommunikationsumständen, da es für interessierte Angreifer leicht möglich ist, die vermittelte „Anonymität“ aufzuheben.[171]

169 Siehe ausführlich zur Funktionsweise von Proxys Wikipedia, Proxy (Rechnernetz), Version vom 04.04.2009, 20.22 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Proxy_(Rechnernetz)&oldid=58680295.

170 Siehe Wikipedia, Anonymizer, Version vom 24.03.2009, 18.28 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Anonymizer&oldid=58270526. Vergleiche auch die Definition von `*anonymizer´* in RFC 4949: Internet Security Glossary, Version 2 vom August 2007, verfügbar unter http://www.heise.de/netze/rfc/rfc s/rfc4949.shtml (29.05.2009), S. 17: „An internetwork service, usually provided via a proxy server, that provides anonymity and privacy for clients. That is, the service enables a client to access servers (a) without allowing anyone to gather information about which servers the client accesses and (b) without allowing the accessed servers to gather information about the client, such as its IP address.“

171 *Pfitzmann/Steinbrecher*, Digitale Glaubwürdigkeit und Privatsphäre in einer vernetzten Gesellschaft, in: *Klumpp/Kubicek/Roßnagel,* Next generation information society?, S. 290, 294.

b. Grundsätze zur Gewährleistung von Anonymität

Für die Gewährleistung verlässlicher, sicherer Anonymität ergeben sich aus dem Gesagten folgende drei Grundsätze für die Vertraulichkeit von Informations- und Kommunikationsverhalten:

- Erstens muss ein vertrauenswürdiges Konzept für Anonymität immer davon ausgehen, dass Datenverkehr abgehört werden kann[172] – da dies jedenfalls möglich und vom Nutzer in keiner Weise abseh- oder kontrollierbar ist.
- Zweitens müssen die Daten beim Vergleich von Dateneingang und Datenausgang eines Vermittlungsrechners das Erscheinungsbild geändert haben – da ansonsten jeder, der diesen Netzwerkverkehr abhört, die Datenpakete anhand des Bitmusters identifizieren und zuordnen könnte.[173]
- Drittens darf ein sicheres Konzept für die Gewährleistung von Anonymität nicht allein auf die Vertrauenswürdigkeit und (IT-sicherheitsrechtliche) Verlässlichkeit nur eines Vermittlers setzen, denn die Ausübung dieser Kontrolle der Vertrauenswürdigkeit und Verlässlichkeit ist dem Nutzer gerade nicht möglich.[174]

c. Sichere Anonymität durch Verschlüsselung

Diese Grundsätze werden maßgeblich durch Verschlüsselung umgesetzt, vor allem bezüglich der Änderung des Erscheinungsbildes der Datenpakete. Dieser Ansatz lebt natürlich davon, dass möglichst viele andere Nutzer gleichzeitig den Dienst nutzen. Um eine Zuordnung von ein- und ausgehendem Datenverkehr zusätzlich zu erschweren, werden teilweise nur Datenpakete identischer Größe versendet, zusätzlicher Datenverkehr geschaffen (durch Versendung weiterer, an sich nicht erforderlicher Datenpakete), etc. Um die Abhängigkeit von der Vertrauenswürdigkeit der einzelnen Vermittlungsrechner zu minimieren, werden verschiedene Vermittlungsrechner hintereinander durchlaufen. Die bekanntesten Anonymisierungsprojekte sind dabei derzeit zum einen das Tor-Netzwerk (Tor ist das Akronym von `*The Onion Routing´*)[175] und zum anderen das Projekt AN.ON (Anonymität.Online)[176] mit der von

172 *Pfitzmann*, Möglichkeiten und Grenzen von Anonymität, in: *Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen,* Datenschutz und Anonymität, S. 9, 12.

173 *Pfitzmann*, Möglichkeiten und Grenzen von Anonymität, in: *Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen,* Datenschutz und Anonymität, S. 9, 12 f.

174 So wird etwa für das Anonymisierungsnetzwerk Tor vermutet, dass auch US-amerikanische, russische und chinesische Regierungskreise Vermittlungsrechner im Tor-Netzwerk betreiben, vor allem solche, die als Endpunkte vor der letztlichen Übermittlung an den Empfänger fungieren (sog. `*exit nodes´*); siehe heise online vom 21.11.2007, Anonymisierungsnetz Tor "abgephisht", Teil 2, verfügbar unter: http://www.heise.de/newsticker/Anonymisierungsnetz-Tor-abgephisht-Teil-2--/meldung/99318 (07.05.2009).

175 Ausführliche Informationen unter http://www.torproject.org/ (07.05.2009).

176 Siehe unter http://anon.inf.tu-dresden.de/index.html (07.05.2009).

ihm entwickelten Software JonDo.[177] Beide Anonymisierungsnetzwerke routen Anfragen über mehrere Vermittlungsrechner hintereinander, die technische Implementierung dieses Hintereinanderschaltens mehrerer Vermittlungsrechner unterscheidet sich aber jeweils.[178] Gemeinsam ist allen Ansätzen, dass die einzelnen Datenpakete jeweils verschlüsselt werden:

Im Tor-Netzwerk werden Datenpakete mehrfach übereinander verschlüsselt, so dass die verschiedenen Verschlüsselungsschichten wie die Häute einer Zwiebel übereinander liegen. Die einzelnen Vermittlungsrechner entschlüsseln jeweils eine verschlüsselte Schicht und leiten die Daten dann weiter.[179] Im Rahmen des Projekts AN.ON werden die Daten dagegen jeweils für einen Vermittlungsschritt verschlüsselt, an den nächsten Vermittlungsrechner übermittelt, dort entschlüsselt, umsortiert und erneut für den nächsten Übermittlungsschritt verschlüsselt.[180] Die Verschlüsselung ist erforderlich, damit die Anonymität durch Abhören des Datenverkehrs nicht aufgehoben werden kann. Alle Systeme, die effektive Vertraulichkeit von Kommunikationsumständen gewährleisten, setzen nach derzeitigem Stand der Technik Verschlüsselungsverfahren ein.[181]

5. Ergebnis

Verschlüsselungsverfahren sind nach dem derzeitigen Stand der Technik die zentrale Technologie zur Gewährleistung der Vertraulichkeit von Kommunikationsinhalten und Kommunikationsumständen. Grundsätzlich ist auch der Einsatz anderer informationstechnischer Verfahren oder Technologien denkbar, um Vertraulichkeit zu sichern. Derzeit verfügen aber Verschlüsselungsverfahren über wesentliche Alleinstellungsmerkmale: Verschlüsselungsverfahren sind die einzigen Verfahren, die ein vielfach geprüftes, hohes Sicherheitsniveau aufweisen. Trotz des hohen Sicherheitsniveaus bleiben diese Verfahren in der alltäglichen Massenanwendung praktisch handhabbar. Diese Kombination von hohem Sicherheitsstandard und Praktikabilität wird derzeit nur durch Verschlüsselungsverfahren verwirklicht. Verschlüsselung ist damit *das* technische Verfahren zur Gewährleistung von Kommunikationsvertraulichkeit.

177 Zur grundlegenden Funktionalität vergleiche http://anon.inf.tu-dresden.de/help/jap_help/de/help/about.html (07.05.2009).

178 Einzelheiten bei *Pfitzmann/Steinbrecher*, Digitale Glaubwürdigkeit und Privatsphäre in einer vernetzten Gesellschaft, in: *Klumpp/Kubicek/Roßnagel,* Next generation information society?, S. 290, 294 f.

179 Eine ausführliche Erklärung vergleiche unter http://hp.kairaven.de/bigb/asurf2.html#a1 (07.05.2009).

180 Einzelheiten unter Wikipedia, Java Anon Proxy, Version vom 03.05.2009, 22.33 Uhr, verfügbar unter: http:// de.wikipedia.org/w/index.php?title=Java_Anon_Proxy&oldid=59680564.

181 Siehe einen Überblick über Anonymisierungsdienste bei *Brunst*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, S. 130 ff.

II. Verschlüsselung und digitale Signatur als Maßnahmen der Integritätssicherung

Neben dem veränderten Bedürfnis nach Vertraulichkeit von Daten hat sich auch der Bedarf an der Sicherung der Integrität von Daten gewandelt.

1. Mangelnder technischer Schutz der Integrität in der digitalen Welt

Die exponentiell angestiegenen Möglichkeiten fremden Zugriffs auf Kommunikationsdaten bergen neben der Gefahr des Abhörens ebenso die Gefahr der Manipulation (Veränderung, Unterdrückung etc.)[182] von internetbasierter Kommunikation. Als Oberbegriff für den Schutz vor allen Arten von Manipulationsgefahren dient der informationstechnische Terminus des Integritätsschutzes. *Integrität* wird häufig[183] als „Schutz vor unbefugter Veränderung von Informationen" definiert.[184] Dementsprechend wird hier der Schutz der *Authentizität* (etwa als „die Echtheit und Glaubwürdigkeit des Objekts bzw. Subjekts, die anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar ist"[185] definiert) als Teil des Integritätsschutzes verstanden:

- Der Schutz vor unbefugter Veränderung von Informationen erfordert zwingend die vorherige Feststellung, ob und in welchem Umfang eine bestimmte Person befugt ist. Dies ist nichts anderes als die *Authentizität von Subjekten*.[186]
- Die *Authentizität von Objekten* wird vor allem bei der Übertragung von Daten über unsichere Transportmedien (etwa das Internet) relevant. Die Authentizitätsforderung verlangt eine Prüfung der Echtheit der Daten im Sinne eines Ursprungs- oder Urhebernachweises.[187] Diese Frage danach, ob die Daten von dem stammen, der als ihr Urheber erscheint, ist beinahe untrennbar mit der Frage nach der Datenintegrität verknüpft. Geht es um eine Veränderung der inhaltlichen Information, ist dies klar eine Frage der Datenintegrität. Geht es um die alleinige Veränderung des Urhebers (Die Daten stammen von A, B lässt die Daten inhaltlich unverändert und manipuliert nur den Urhebernachweis, so dass jetzt B als Urheber erscheint.), ist dies aber ebenfalls eine Frage der Datenintegrität: Die Information über die Urheberschaft ist Bestandteil der Daten und nimmt insoweit am Integritätsschutz teil. Das Beispiel zeigt gerade, dass Authentizität und Integrität nicht zu trennen sind: Die Veränderung des Urhebers durch B stellt eine Integritätsverletzung dar; der unbefugte B hat die Daten verändert.

182 Vgl. zur Terminologie oben unter 1.b.bb).
183 Siehe zur diesbezüglichen terminologischen und folglich auch definitorischen Vielfalt sogleich unter III.
184 So auch Ziffer 0.2 Information Technology Security Evaluation Criteria (ITSEC); verfügbar unter: http://www.bsi.de/zertifiz/ itkrit/itsec-dt.pdf (13.02.2008).
185 *Eckert*, IT-Sicherheit, S. 6 f.
186 Die Authentizität von Subjekten ist derzeit der zentrale Aspekt im Rahmen der Authentizität; vgl. dazu *Eckert*, IT-Sicherheit, S. 7.
187 *Eckert*, IT-Sicherheit, S. 7.

Ein Bedarf des Schutzes der Integrität besteht dabei sowohl für Daten bei (internetbasierter) Kommunikation (a.) als auch für alle Arten von Daten, die manipulationssicher gespeichert werden sollen (b.).

a. Technikbedingt fehlende Integrität von Kommunikationsinhalten und Kommunikationsumständen

Es ist offensichtlich, dass E-Mails, die technikbedingt von jedem Interessierten abgefangen und mitgelesen werden können, ebenso mühelos verändert oder unterdrückt werden können:

> „Zudem können E-Mails mit wenig Aufwand auf dem Weg abgefangen, wie Postkarten mitgelesen und in ihrem Inhalt verändert werden. Sender und Empfänger können nie sicher sein, mit wem sie gerade tatsächlich kommunizieren. Identitätsdiebstahl wird zu einem wachsenden und weithin ungelösten Problem."[188]

- So ist es beispielsweise leicht möglich, eine E-Mail zu versenden unter Angabe einer Absenderadresse, die einem Dritten gehört oder gar nicht existiert (sog. `*Mail Spoofing*´).[189] Spam-Mails werden häufig unter fremden oder inexistenten Absenderadressen verschickt. Phishing-Mails versuchen ebenfalls häufig, unter Verwendung fremder Absenderadressen dem Empfänger vorzutäuschen, die E-Mail stamme von einem anderen als dem tatsächlichen Absender (zumeist von Banken, Bezahlsystemen, Versand- oder Online-Auktionshäusern), damit die Empfänger letztlich geheim zu haltende, persönliche Zugangsdaten preisgeben.[190] Jedem können damit unter seiner E-Mail-Adresse scheinbar von ihm stammende Äußerungen untergeschoben werden. Umgekehrt kann sich kein Empfänger einer E-Mail darauf verlassen, dass die E-Mail tatsächlich von der Person herrührt, die als Absender firmiert.
- Angreifer können E-Mails auch vollständig verschwinden lassen, so dass diese gar nicht ihren Adressaten erreichen. Daten können gezielt umgeleitet und somit auch unterdrückt werden.[191]
- Vor allem aber kann der Inhalt von E-Mails beliebig durch Dritte verändert werden. Wer Zugriff auf Daten hat, kann diese grundsätzlich auch verändern und dann in manipuliertem Zustand weiterleiten.[192]

188 Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung, Bürgerportale, verfügbar unter: http://www.kbst.bund.de/nn_836958/Content/Egov/Bportale/bportale.html__nnn =true (19.09.2008).

189 Wikipedia, Mail-Spoofing, Version vom 08.01.2009, 22.33 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Mail-Spoofing&oldid=55087807; *Brands*, IT-Sicherheitsmanagement, S. 140.

190 Einzelheiten siehe unter Wikipedia, Phishing, Version vom 02.05.2009, 04.22 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Phishing&oldid=59620936.

191 Siehe zu den Möglichkeiten der Wegemanipulation *Brands*, IT-Sicherheitsmanagement, S. 79 ff., 85.

Internetbasierte Kommunikation gewährleistet somit keinerlei Integrität der Daten. Dies ist zwingende Folge der Architektur des Internets.[193] Gleiches gilt auch für alle sonstigen Datenübermittlungen über Netze. Netze sind konstruktionsbedingt (s.o. unter I.1.b.) Umgebungen, die Manipulationen der Daten gestatten. Das Verhindern von Manipulation ist konstruktionsbedingt unmöglich.[194] Daher werden Netze auch als so genannte `*unsichere Umgebungen*´ bezeichnet.

b. Technikbedingt reduzierte Integrität sonstiger Daten

Im Gegensatz dazu werden Umgebungen, in denen Manipulationen *von vornherein verhindert* werden können, als so genannte `*sichere Umgebungen*´ bezeichnet (Da es absolute Sicherheit nicht geben kann, wäre `absicherbare Umgebung´ vielleicht die präzisere Bezeichnung – es bleibt aber bei der Verwendung der allgemein üblichen Terminologie).

Auch in solchen (vermeintlich) sicheren Umgebungen ist die Integrität von Daten nur bedingt gewährleistet. Gleichzeitig besteht für eine Vielzahl von Daten der Bedarf, diese sicher vor Veränderung und/oder vor Verlust zu speichern. Daten sind dabei – etwa im Vergleich zu Dokumenten in Papierform – viel anfälliger dafür, unbefugt gelöscht oder unbemerkt manipuliert zu werden.

- Ein körperlicher Zugriff wie bei einem Schriftstück ist häufig nicht erforderlich, da ein Großteil von Rechnern über eine Internetverbindung verfügt. Sobald ein informationstechnisches System über einen Internetzugang verfügt, können Dritte dieses System (häufig auch unbemerkt) infiltrieren und Daten spurenlos löschen oder unbemerkt verändern. Über derartige Möglichkeiten der Infiltration informationstechnischer Systeme ist gerade im Rahmen der geplanten Einführung von Befugnissen zur Online-Durchsuchung durch das BKA sowie im Urteil des BVerfG[195] zu einer entsprechenden Rechtgrundlage in Nordrhein-Westfalen (§ 5 II Nr. 11 VSG-NW a.F.[196]) viel diskutiert worden. Die Vorgehensweise krimineller Privatpersonen und die staatlicher Sicherheitsbehörden im Rahmen der Online-Durchsuchung stimmen insoweit überein.[197]
- Technisch kann eine Infiltration[198] durch Dritte im Wesentlichen auf zwei Wegen erfolgen:[199] Zum einen kann der Nutzer eines informationstechnischen Sys-

192 Lohnenswert ist dies aus Sicht des Angreifers zumeist aber nur dann, wenn die Daten von ihm interpretierbar sind und er daher weiß, was er verändert; *Brands*, IT-Sicherheitsmanagement, S. 37.
193 Siehe oben unter 1.a.
194 *Eckert*, IT-Sicherheit, S. 8.
195 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07.
196 Verfassungsschutzgesetz Nordrhein-Westfalen i.d.F.v. 20.12.2006.
197 *Hansen/Pfitzmann/Roßnagel,* DRiZ 2007, 225, 227.
198 Siehe ausführlich zur Infiltration durch Trojaner *Hartmann*, Sichere Kommunikation im Internet, S. 89 ff.

tems – durch Hinweise auf angebliche Rechnungen, Strafanzeigen, pornographische Inhalte usw. – verleitet werden, Dateianhänge von E-Mails zu öffnen, die einen Trojaner enthalten, oder entsprechende Dateien aus dem Internet herunterzuladen und auszuführen.[200] Zum anderen können gezielt Sicherheitslücken von Programmen oder Betriebssystemen ausgenutzt werden. Informationen über derartige Sicherheitslücken werden via Internet gehandelt und können von Interessierten erworben werden.[201] Es ist absehbar, dass es immer Sicherheitslücken in Software geben wird. Die Programme werden zwar überarbeitet, verbessert und gepatcht, gleichzeitig werden aber auch immer neue Nachfolgeversionen mit erhöhter Funktionalität entwickelt, die wiederum neue *`bugs´* und Sicherheitslücken enthalten.[202] Zudem gibt es einen erheblichen Anteil an bekannten Sicherheitslücken, für die gleichwohl kein Patch existiert.[203]

- Selbst wenn der Nutzer gängige Sicherheitsmaßnahmen (Firewall, Virenscanner etc.) getroffen hat, seine Software regelmäßig aktualisiert und hinsichtlich bekannter Infiltrationswege (E-Mail-Anhänge usw.) misstrauisch ist, schützt ihn dies nur vor den plumpesten Angriffen. Wird ein sog. *`Less-Than-Zero-Day Exploit´*, d.h. ein Angriffsprogramm, das bisher unbekannte und unveröffentlichte

199 Je nach verfügbaren Ressourcen sind aber ebenso ein Zuspielen von Hardware mit dem entsprechenden Programm, eine manuelle Installation bei direktem physischem Zugriff auf das informationstechnische System oder der Einbau einer „Hintertür“ in Software möglich. Privater Dritter kann nicht nur ein Krimineller (und auch dieser kann über beträchtliche Ressourcen verfügen, insbesondere im Bereich der Organisierten Kriminalität), sondern auch ein ausländischer Geheimdienst sein. Die im Folgenden genannten Infiltrationsmöglichkeiten wurden lediglich herausgegriffen, da es sich hierbei um die verbreitetesten Massenangriffe handelt; ebenso *Buermeyer,* HRRS 2007, 154, 156.

200 *Hansen/Pfitzmann/Roßnagel,* DRiZ 2007, 225, 227; Fox, Stellungnahme zur "Online-Durchsuchung", verfügbar unter: http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf (30.12.2008), S. 6. Sicherheitsexperten gehen davon aus, dass jeder Internetnutzer täglich mit Trojaner-Programmen bombardiert wird, vgl. heise online vom 27.08.2007, Online-Spionage `alltäglicher Wahnsinn des Internet´, http://www.heise.de/newsticker/meldung/94980 (03.09.2007).

201 *Hansen/Pfitzmann/Roßnagel,* DRiZ 2007, 225, 227; Fox, Stellungnahme zur "Online-Durchsuchung", verfügbar unter: http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf (30.12.2008), S. 6; *Pohl,* DuD 2007, 684, 685. Vgl. dazu auch heise online vom 10.06.2008, Trojanerbaukasten mit Rund-um-die-Uhr-Support und Austausch-Service, verfügbar unter: http://www.heise.de/newsticker/Trojanerbaukasten-mit-Rund-um-die-Uhr-Support-und-Austausch-Service--/meldung/109254 (11.06.2008).

202 Zu diesem von ihm so bezeichneten „Software-Problem“ ausführlich *Brands*, IT-Sicherheitsmanagement, S. 12 ff.

203 Laut heise online vom 03.02.2009, Studie: Viele Sicherheitslücken bleiben ungepatcht, verfügbar unter: http: //www.heise.de/newsticker/Studie-Viele-Sicherheitsluecken-bleiben-ungepatcht--/meldung/126785 (03.02.2009) gab es für 53 Prozent der im Jahr 2008 bekannt gewordenen Sicherheitslücken keine Patches und 44 Prozent der im Vorjahr veröffentlichten Lücken blieben weiterhin ungepatcht. Dabei können laut Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2009, verfügbar unter: http://www.bsi.bund.de/literat/lagebericht/Lagebericht2009.pdf (09.03.2009), S. 19 drei Viertel der entdeckten Schwachstellen tatsächlich von einem entfernten Angreifer ausgenutzt werden.

Sicherheitslücken ausnutzt,[204] eingesetzt, ist nur ein physisch gänzlich von anderen informationstechnischen Systemen, Internet und Intranets losgelöstes System (sog. *`stand-alone´*-System) davor sicher.[205] Einen derartigen (organisatorischen, aber auch finanziellen) Aufwand wird kaum ein Nutzer zu treffen bereit sein. Selbst bei Umsetzung eines solchen Sicherheitskonzepts können logischerweise nur solche Daten durch Systemtrennung geschützt werden, die nicht mit der Nutzung des Internets in Zusammenhang stehen: E-Mails befinden sich notwendigerweise auf einem System *mit* Internetanbindung, gleiches gilt für alle Daten, die mit irgendwelchen Internetanwendungen in Verbindung stehen (Online-Banking, Steuerdaten (ELSTER), etc.). Einzelne Teilbereiche können damit zwar durchaus erfolgreich durch ein Konzept der Systemtrennung geschützt werden, alle Daten, die irgendwie mit Internetnutzung zusammenhängen, können auf diesem Weg aber nicht geschützt werden.

- Schließlich kann auch die Ausnutzung von sog. *`Zero-Day Exploits´* (die bekannte, aber noch nicht gepatchte Sicherheitslücken ausnutzen und daher zum einen billiger und zum anderen einem breiteren Personenkreis zugänglich sein dürften) jeden Nutzer treffen, sei er noch so umsichtig. Niemand kann immer von jeder Sicherheitslücke wissen[206] und sich entsprechend schützen– insbesondere wenn eine Lücke zwar veröffentlicht ist, aber noch kein Patch entwickelt wurde.[207]

Folglich besteht grundsätzlich in allen informationstechnischen Systemen, die über eine Internetverbindung verfügen, die Gefahr der Verletzung der Datenintegrität. Diese Integritätsgefahren sind qualitativ und quantitativ bedrohlicher als dies bei nicht-digitalen Schriftstücken, Dokumenten u.ä. der Fall ist. Informationstechnische Systeme, die keinerlei Verbindung zum Internet aufweisen, können im Wege direkten, körperlichen Zugriffs ebenfalls infiltriert werden. Insoweit bestehen allerdings im Vergleich zu nicht-digitalen, körperlichen Schriftstücken keine signifikanten Unterschiede des Gefährdungsniveaus. Ein Konzept der strikten Trennung von informationstechnischen Systemen ist allerdings die Ausnahme und nicht die Regel.

204 Ausführlich dazu *Pohl,* DuD 2007, 684, 685; Gesellschaft für Informatik e.V., Pressemitteilung vom 30.08. 2007, verfügbar unter: http://www.gi-ev.de/aktuelles/meldungsdetails/meldung/167/ (26.05.2008).

205 *Pohl,* DuD 2007, 684, 687.

206 Wie die Bezeichnung *`Zero-Day Exploit´* verdeutlicht, werden dabei Sicherheitslücken unmittelbar nach deren Veröffentlichung (häufig noch am selben Tag) für Angriffe ausgenutzt; *Pohl,* DuD 2007, 684, 685.

207 *Pohl,* DuD 2007, 684, 687. Ein Beispiel aus der jüngeren Vergangenheit, das zugleich zeigt, wie wenig sich der Einzelne teilweise selbst schützen kann, ist ein *`Zero-Day Exploit´*, der sich gegen eine Lücke in allen Versionen des Internet Explorers richtete. Auch auf den Internetseiten vertrauenswürdiger Anbieter konnte man sich mit dem *Exploit* infizieren. Solange kein Patch existierte konnte als Schutzmaßnahme nur ein anderer Browser genutzt werden; vgl. heise online vom 13.12.2008, Zero-Day-Exploit für Internet Explorer breitet sich aus, verfügbar unter: http://www.heise.de/security/Zero-Day-Exploit-fuer-Internet-Explorer-breitet-sich-aus--/news/meldung/120388 (02.01.2009).

Für den Großteil informationstechnischer Systeme und darauf gespeicherter Daten bestehen signifikant angestiegene Integritätsgefahren. Dies zeigt, dass selbst ein an sich als `sichere Umgebung´ klassifiziertes einzelnes informationstechnisches System nicht `sicher´ ist, sondern allenfalls sicherbar.

2. Gestiegene Notwendigkeit der Gewährleistung von Integrität in der digitalen Welt

Mit der zunehmenden Digitalisierung privater, geschäftlicher und behördlicher Kontakte besteht eine gestiegene Notwendigkeit, dass Daten manipulationssicher übermittelt und gespeichert werden können und die Identität von Kommunikationspartnern sichergestellt werden kann. Sicherungen, die bei herkömmlicher telefonischer oder postalischer Kommunikation gegeben sind, existieren oder wirken nicht in gleicher Weise bei internetbasierter Kommunikation:

- Internetkommunikation wird nicht durch in besonderem Maße vertrauenswürdige *Transportmittler* wie die Post bzw. deren Nachfolgeunternehmen übermittelt, sondern *jeder* kann einen Router betreiben.
- Ein Zugriff auf Kommunikationsdaten im Internet kann *von jedem Ort der Welt* durchgeführt werden und ist ohne körperlichen Zugriff möglich, so dass sowohl Entdeckungs- wie auch Verfolgungsrisiko sinken, während sich der Kreis potentieller Angreifer erweitert.
- Wichtige *Authentifizierungsmerkmale fallen weg* oder werden in ihrer Zuverlässigkeit stark geschwächt. So existiert zunächst für die E-Mail kein Äquivalent zur handschriftlichen Unterschrift auf einem Brief. Die Stimme kann zwar bei Internet-Telefonie im gleichen Maße wie bei einem hergebrachten Telefongespräch als Authentifizierungsmerkmal dienen. Durch die digitale, paketbasierte Übermittlung ergeben sich aber erhebliche Manipulationsmöglichkeiten, die bei einem herkömmlichen Telefonat nicht existieren. Digitale Sprachdaten können unterdrückt, gespeichert, bearbeitet, wieder eingespielt usw. werden.

3. Verschlüsselung und digitale Signatur zur Gewährleistung der Integrität

Auch der Schutz der Integrität von Daten wird durch Verschlüsselungsverfahren gewährleistet, teilweise durch Verschlüsselung, teilweise durch Signatur- und insbesondere Hashverfahren. Dabei ist zwischen den so genannten `sicheren´ und `unsicheren´ Umgebungen zu unterscheiden:

- Als `*unsicher´* werden danach Umgebungen bezeichnet, in denen Manipulationen der Daten nicht von vornherein verhindert werden können. Klassisches Beispiel sind Netze, insbesondere das Internet.
- Als `*sicher´* werden demgegenüber Umgebungen bezeichnet, in denen eine Manipulationsverhinderung grundsätzlich möglich erscheint. Beispiele sind etwa ein völlig alleinstehendes informationstechnisches System (sog. `*stand-alone´*-

System) oder ein informationstechnisches System, das gegenüber anderen Systemen abgeschottet bzw. geschützt ist.

Die Unterscheidung des Integritätsschutzes in sog. sicheren und unsicheren Umgebungen beruht darauf, dass das angestrebte Schutzniveau unterschiedlich sein muss:

- Geht es um die Integrität von Daten in sog. sicheren Umgebungen, kann und soll regelmäßig *jede unbefugte* Veränderung von Daten verhindert werden.
- Geht es dagegen um die Integrität von Daten in unsicheren Umgebungen – etwa in per se manipulationsanfälligen Netzen – kann eine unbefugte Veränderung konstruktionsbedingt nicht verhindert werden. Das Schutzziel muss daher sein, zumindest eine *unbemerkte* unbefugte Veränderung zu verhindern.[208]

a. Integritätsschutz in sog. `sicheren Umgebungen´

In sicheren Umgebungen kann und soll jede unbefugte Veränderung von Daten verhindert werden. Es handelt sich um ein Schutzkonzept der *Verhinderung* von unbefugter Datenveränderung.

aa) Rechteverwaltung

Die Integrität von Daten wird durch Maßnahmen der Rechteverwaltung und Zugriffskontrolle gewährleistet.[209] Erforderlich ist die individuelle Vergabe von Rechten zur Nutzung von Daten an alle Nutzer (etwa Schreib- oder Leseberechtigungen).

> „Die Rechteverwaltung hat zu gewährleisten, dass alle Subjekte und Objekte fälschungssicher identifiziert werden und dass jedes Objekt, für das Zugriffsbeschränkungen festgelegt sind, auch wirklich von der Rechteverwaltung erfasst wird.“[210]

Jeder Zugriffsversuch muss kontrolliert werden; es darf keine Umgehungsmöglichkeiten der Kontrolle geben (Zugriffskontrolle).[211] Technisch werden diese Ziele durch ein komplexes Zusammenspiel verschiedener hardware- und softwarebasierter Kontrollsysteme verwirklicht. Verschlüsselungsverfahren sind dabei in jedem Fall zur Gewährleistung der sicheren Speicherung der Informationen über die einzelnen Berechtigungen einzusetzen.[212]

208 So dazu *Eckert*, IT-Sicherheit, S. 8.
209 *Eckert*, IT-Sicherheit, S. 8.
210 *Eckert*, IT-Sicherheit, S. 535 f.
211 *Eckert*, IT-Sicherheit, S. 536.
212 *Eckert*, IT-Sicherheit, S. 545; *Gola/Schomerus,* BDSG, § 9, Rn. 13.

bb) Authentifikation

Die Wirksamkeit der Rechteverwaltung basiert weiter darauf, dass alle Objekte und vor allem Subjekte (die Nutzer) sicher identifiziert werden. *Die Verwirklichung des Schutzziels der Authentizität ist notwendige Voraussetzung für die Realisierung des Schutzziels der Integrität*. Je nachdem, welcher Typ von Authentifikationsverfahren eingesetzt wird, ist auch hier die Verwendung von Verschlüsselungsverfahren unabdingbar. Authentifikationsverfahren können in drei Kategorien eingeteilt werden: Wissensbasierte Authentifikation, besitzbasierte Authentifikation und eigenschaftsbasierte Authentifikation.[213]

- Bei der wissensbasierten Authentifikation werden Subjekte durch die Kenntnis eines Geheimnisses identifiziert. Häufigste Variante ist die Kenntnis eines Passworts,[214] etwas komplexer sind Frage-Antwort-Protokolle (*`challenge-response´*-Verfahren[215]) wie etwa das PIN/TAN-Verfahren.[216] Die Sicherheit der Passwörter vor unbefugter Kenntnisnahme ist zwingend durch Verschlüsselungsverfahren zu gewährleisten.[217]
- Die besitzbasierte Authentifikation bezieht sich zumeist auf den Besitz einer *`smart card´*[218] oder – zunehmend - eines USB-Tokens.[219] Daneben benötigt der Benutzer regelmäßig auch spezielles Wissen – zumeist in Form einer PIN. [220] Verschlüsselungsverfahren werden häufig genutzt, um die auf der Smartcard gespeicherte PIN zu schützen. Jedenfalls für den nachfolgenden zweiten Schritt innerhalb des Authentifizierungsverfahrens, der Authentifikation zwischen der

213 Für einen kurzen Überblick vergleiche *Albrecht*, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, S. 32 f.

214 *Eckert*, IT-Sicherheit, S. 432 ff.

215 Vergleiche die Definition von `challenge-response´ in RFC 4949: Internet Security Glossary, Version 2 vom August 2007, verfügbar unter: http://www.heise.de/netze/rfc/rfcs/rfc4949.shtml (29.05.2009), S. 58: „An authentication process that verifies an identity by requiring correct authentication information to be provided in response to a challenge. In a computer system, the authentication information is usually a value that is required to be computed in response to an unpredictable challenge value, but it might be just a password."

216 *Eckert*, IT-Sicherheit, S. 451 ff.

217 *Eckert*, IT-Sicherheit, S. 432. Die kryptographische Sicherheit der Passwörter allein reicht natürlich noch nicht aus, das Passwort muss auch sinnvoll gewählt sein (und nicht etwa durch eine simple Wörterbuchattacke zu erraten sein), das Sicherheitsbewusstsein der Nutzer zum Umgang mit Passwörtern muss entsprechend ausgeprägt sein, usw.; *Eckert*, IT-Sicherheit, S. 433.

218 Eine *`smart card´* wird definiert als "A credit-card sized device containing one or more integrated circuit chips that perform the functions of a computer's central processor, memory, and input/output interface."; RFC 4949: Internet Security Glossary, Version 2 vom August 2007, verfügbar unter http://www.heise.de/netze/rfc/rfcs/rfc49 49.shtml (29.05.2009), S. 285.

219 *Eckert*, IT-Sicherheit, S. 458. Unter einem *`token´* versteht man „A data object or a physical device used to verify an identity in an authentication process."; RFC 4949: Internet Security Glossary, Version 2 vom August 2007, verfügbar unter http://www.heise.de/netze/rfc/rfcs/rfc4949.shtml (29.05.2009), S. 307.

220 *Eckert*, IT-Sicherheit, S. 468.

Smartcard und dem Zielsystem, werden zwingend Verschlüsselungsverfahren eingesetzt in Form von `*challenge-response*´-Protokollen.[221]

- Die eigenschaftsbasierte Authentifikation beruht auf biometrischen Merkmalen, die entweder physiologisch (Iris, Fingerabdruck) oder verhaltenstypisch (spezifischer Rhythmus, Anschlag usw. bei Tastaturangaben, die handschriftliche Unterschrift) sein können.[222] Es ist das einzige Authentifikationsverfahren, das nicht zwingend auf den Einsatz von Verschlüsselung angewiesen ist.[223]

Soweit es um mobile Endgeräte (wie Laptops, PDAs etc.) geht, muss außerdem für den Fall der Umgehung der Zugriffskontrollen des Betriebssystems vorgesorgt werden.[224] Dazu empfiehlt sich der Einsatz von verschlüsselnden Dateisystemen.[225] Zur Gewährleistung der Datenintegrität in sog. sicheren Umgebungen ist somit zwingend der Einsatz von Verschlüsselungsverfahren erforderlich.

b. Integritätsschutz in sog. `unsicheren Umgebungen´

Wie bereits dargestellt, kann in unsicheren Umgebungen (etwa Netzen wie dem Internet) ein Schutz vor unbefugter Veränderung von Daten nicht gewährleistet werden. Da eine Verhinderung der unbefugten Veränderung von Daten nicht möglich ist, zielt das Schutzkonzept daher auf die *Feststellung* der unbefugten Veränderung von Daten (Schutz vor unbemerkter unbefugter Veränderung).

aa) Hashfunktionen

Zum Schutz vor unbemerkter Veränderung von Daten werden Hashfunktionen, und damit ebenfalls Verschlüsselungsverfahren eingesetzt: Um unbemerkte Veränderungen beispielsweise einer Datei im Nachhinein feststellen zu können, wird der Hashwert der Datei berechnet und mit dieser zusammen gespeichert[226] oder übermittelt. Berechnet man zu einem späteren Zeitpunkt den Hashwert der Datei erneut und

221 *Eckert*, IT-Sicherheit, S. 469.

222 *Eckert*, IT-Sicherheit, S. 473. Ausführlich zu biometrischen Verfahren *Albrecht*, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, S. 39 ff.

223 Zu möglichen Schwachstellen, die im Zusammenhang mit der Nutzung biometrischer Merkmale zur Authentifikation auftreten können, und deren Behebung (etwa durch Verschlüsselungsverfahren), siehe *Eckert*, IT-Sicherheit, S. 487. Vgl. im Übrigen zum Zusammenspiel von Biometrie und Verschlüsselung *Albrecht*, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, S. 58 f.

224 Diese und weitere Anforderungen bei der Verarbeitung personenbezogener Daten auf tragbaren Rechnern aufstellend *Gola/Schomerus,* BDSG, § 9, Rn. 17.

225 Siehe dazu ausführlich *Eckert*, IT-Sicherheit, S. 576 ff.

226 Hashfunktionen werden auch zum Integritätsschutz in sicheren Umgebungen verwendet; *Eckert*, IT-Sicherheit, S. 350.

stimmt er mit dem gespeicherten oder ebenfalls übermittelten Hashwert überein, dann kann davon ausgegangen werden, dass die Datei in der Zwischenzeit nicht verändert wurde.[227] Eine veränderte Datei hätte zu einem anderen Hashwert geführt. Aufgrund der oben (siehe unter A.IV.3.) geforderten Kollisionseigenschaften von sicheren Hashfunktionen kann auch praktisch ausgeschlossen werden, dass ein Angreifer eine andere Ursprungsdatei finden kann, die auf denselben Hashwert abgebildet wird (Kollisionsresistenz).

bb) `Message Authentication Code´

Damit ein Angreifer nicht sowohl die zu schützende Datei selbst als auch deren Hashwert manipulieren kann, muss zur Sicherstellung der Integrität auch die Authentizität des Erstellers der Datei gewährleistet sein.

Andernfalls könnte ein Angreifer die zu schützende Datei verändern und einfach deren Hashwert an Stelle des ursprünglichen Hashwerts speichern bzw. übermitteln.[228] Eine Geheimhaltung der verwendeten Hashfunktion stellt insoweit keine Alternative dar. Zum einen erschwert es den Einsatz von Hashfunktionen, wenn eine Vereinbarung darüber, welche Funktion verwendet wird, jeweils gesondert getroffen werden muss. Zum zweiten sollte die Sicherheit eines Systems niemals allein auf Geheimhaltung bzw. Verschleierung beruhen, da sich dies bereits häufig als ungenügend erwiesen hat.[229] Dies gilt umso mehr, je bekannter das „Geheimnis“ ist. Letzteres trifft nämlich, zum dritten, gerade auch auf Hashfunktionen zu: Diese werden für viele Zwecke eingesetzt und sind weit verbreitet und bekannt. Wird eine gängige Hashfunktion verwendet, bringt die Geheimhaltung der verwendeten Funktion somit keinerlei realen Sicherheitsgewinn. Wird eine neue, selbst entwickelte Hashfunktion verwendet, birgt dies die Gefahren jedes durch Geheimhaltung „geschützten“ Algorithmus‘: Schwachstellen werden erst entdeckt, wenn das Verfahren bereits verwendet wurde und damit wird im Nachhinein unsicher und nicht mehr vertrauenswürdig, worauf man vorher vertraut hat. Wird ein Algorithmus dagegen offengelegt und erweist sich gegenüber Angriffen von Experten resistent, sinkt die Gefahr, dass im Nachhinein plötzlich Sicherheitslücken entdeckt werden.[230]

Zur Gewährleistung der Authentizität des Erstellers wird in der Regel ein so genannter *`Message Authentication Code´* (MAC) verwendet.[231] Es handelt sich dabei

227 *Eckert*, IT-Sicherheit, S. 350.

228 Siehe *Eckert*, IT-Sicherheit, S. 357.

229 Vgl. Wikipedia, Security through obscurity, Version vom 22.12.2008, 23.06 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?oldid=54452224.

230 Siehe dazu nochmal Wikipedia, Security through obscurity, Version vom 22.12.2008, 23.06 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?oldid=54452224 sowie Wikipedia, Kerckhoffs’ Prinzip, Version vom 10.12.2008, 10.19 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?oldid=53966143.

231 Siehe zu *`Message Authentication Code´ Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 145 f.

um eine Hashfunktion, die zusätzlich noch einen geheimen Schlüssel[232] verwendet. Mit Hilfe des geheimen Schlüssels wird ein Prüfteil generiert und der Datei hinzugefügt. Berechtigte, die den geheimen Schlüssel kennen, können den MAC ebenfalls berechnen und bei Übereinstimmung der beiden MACs sicher sein, dass die Daten vom Berechtigten herrühren und nicht manipuliert wurden.[233]

Der Integritätsschutz in unsicheren Umgebungen erfordert also auch die Gewährleistung der Authentizität des Urhebers der zu schützenden Daten. Diese können nach derzeitigem Stand der Technik nur Verschlüsselungsverfahren gewährleisten.

4. Ergebnis

Der Einsatz von Verschlüsselungsverfahren ist zur Gewährleistung der Integrität von Daten erforderlich, sei es in sog. sicheren oder unsicheren Umgebungen. Der Schutz der Integrität ist dabei jeweils eng mit der Gewährleistung der Authentizität von Subjekten verknüpft. Integrität bedeutet Schutz vor unbefugter Veränderung; zur Feststellung vorhandener oder nicht vorhandener Befugnis ist denknotwenig eine vorherige zuverlässige Authentifizierung der Benutzer erforderlich. Die Notwendigkeit des Einsatzes von Verschlüsselungsverfahren ergibt sich dabei zum Teil aus dem Integritätserfordernis, zum Teil aus dem daraus resultierenden Authentizitätserfordernis. Im Ergebnis sind Verschlüsselungsverfahren nach dem Stand der Technik erforderlich, um die Integrität von Daten sicherzustellen.

III. Verschlüsselung als Kerntechnologie der IT-Sicherheit

Verschlüsselungsverfahren gewährleisten mit dem Schutz der Vertraulichkeit und der Integrität von Daten Kernziele der IT-Sicherheit.

232 Im Rahmen des MAC gibt es *einen* geheimen Schlüssel, der von allen Berechtigten verwendet wird. Damit gibt der MAC gerade keine Auskunft darüber, wer Urheber einer Datei ist. Denn alle Berechtigten können den MAC generieren, da symmetrische kryptographische Schlüssel verwendet werden.

233 Siehe dazu ausführlich *Eckert*, IT-Sicherheit, S. 357 ff.; Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, M 3.23 Einführung in kryptographische Grundbegriffe, verfügbar unter: http://www. bsi.bund.de/gshb/deutsch/m/m03023.htm (07.01.2009) sowie Wikipedia, Message Authentication Code, Version vom 28.12.2008, 12.26 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?oldid=54623381.

1. Informationstechnische Definition der IT-Sicherheit

Dabei kann zunächst festgestellt werden, dass der Begriff der IT-Sicherheit ebenso weit verbreitet[234] wie wenig kohärent definiert und konturiert ist:[235]

> "Begriffsauffassungen zum Thema Sicherheit in der Informationstechnologie gibt es viele."[236]

a. Orientierung an Schutzzielen

Einigkeit herrscht aber zumindest insoweit, als IT-Sicherheit über einen Katalog an so genannten Schutzzielen definiert wird: Sicherheit allein kann als anzustrebender Zustand nicht beschrieben oder konkretisiert werden, da Sicherheit immer *Sicherheit vor* bestimmten Schäden oder Bedrohungen bedeutet (vgl. zur Relativität des Sicherheitsbegriffs oben unter A.III.1.). Da das Vorliegen von Sicherheit relativ zum Vorhandensein von Risiken ist, kommt der Bestimmung möglicher Schäden bzw. Bedrohungen besondere Bedeutung zu. Aus der „Kombination der Wahrscheinlichkeit des Auftretens eines Schadens und des Schweregrades dieses Schadens"[237] ergibt sich das Risiko. Schäden und Risiken können aber nur festgestellt und benannt werden, wenn Klarheit darüber herrscht, welcher Zustand angestrebt wird. Da der Sicherheitsbegriff in seiner Determinierung durch die „Risiken" als Beschreibung des angestrebten Zustandes untauglich ist, wird versucht, das Hauptziel Sicherheit durch die Benennung einzelner so genannter Schutzziele zu konkretisieren.

Darüber, welche Schutzziele im Einzelnen den Begriff der IT-Sicherheit ausmachen, gibt es dann aber viele Auffassungen.[238] Der Diskurs ist dabei von der Verwendung einer Vielzahl unterschiedlicher Begriffe, mangelnder Definition dieser Begriffe, fehlender Konturierung und Abgrenzung sowie oftmals dem Fehlen der Auseinandersetzung mit den von anderen Autoren vorgeschlagenen Schutzzielkatalogen geprägt. Unterschiedliche Schutzzielkataloge, die teils identische, teils abweichende Begriffe und Definitionen enthalten, stehen so nebeneinander – häufig ohne inhaltliche Erläuterung, Auseinandersetzung mit anderen Auffassungen oder Begründung:

234 Eine gute Übersicht bieten *Federrath/Pfitzmann,* DuD 2000, 704.

235 So auch *Eckert*, IT-Sicherheit, S. 1; *Hammer*, Die 2. Dimension der IT-Sicherheit, S. 100 m.w.N.

236 *Raepple*, Sicherheitskonzepte für das Internet, S. 3.

237 Definition von „Risiko" gem. ISO/IEC Guide 51:1999: Safety aspects -- Guidelines for their inclusion in standards, Definition 3.2, zitiert nach: Voges, Definitionen von Begriffen im Kontext ‚Sicherheit (safety)', Vortrag im Rahmen des GI-Workshop zum fachlichen Zusammenhang der Fachgruppen im neuen Fachbereich "Sicherheit" am 12.02.2002, verfügbar unter: http://www11.informatik.uni-erlangen.de/Aktuelles/Veranstaltungen/Sicherheit1/PositionPapers/Voges.pdf (13.02.2008).

238 Einen guten Überblick über verschiedene Schutzzielkataloge und Definitionen bieten *Federrath/Pfitzmann,* DuD 2000, 704.

- So werden zwar teilweise identische Begriffe verwendet, Inhalt und Grenzen der Begriffe differieren aber je nach Autor.[239]
- Die Schutzziele sind häufig nicht trennscharf gegeneinander abgrenzbar. Einzelne Unterkategorein können etwa mehreren übergeordneten Schutzzielen zugeordnet werden, so dass es zu Überlappungen der Schutzziele kommt.[240] So kommt es zum Beispiel sowohl im Rahmen des Schutzes vor unbefugter Preisgabe von Informationen (Vertraulichkeit) als auch im Rahmen des Schutzes vor unbefugter Veränderung von Informationen (Integrität) auf die Feststellung der Unbefugtheit, also die Authentizität, an. Die Unterkategorie `Authentizität´ kann damit sowohl dem Schutzziel Vertraulichkeit als auch dem Schutzziel Integrität zugeordnet werden.
- Teilweise werden Maßnahmen, die bereits der Umsetzung eines oder mehrerer Schutzziele dienen,[241] selbst als Schutzziel definiert. So wird teilweise die Authentizität als eigenes Schutzziel genannt.[242] Authentizität ist aber auch Voraussetzung und Teilaspekt von Integrität (s.o. unter II.1.).[243] Ein weiteres Beispiel ist die Zugriffskontrolle, die von manchen Stimmen als eigenes Schutzziel angesehen wird.[244] Andererseits kann die Zugriffskontrolle auch als Teilaspekt der Integrität verstanden werden. Anonymität – als letztes Beispiel – wird teilweise als eigenständiges Schutzziel definiert, stellt aber auch einen Teilaspekt von Vertraulichkeit dar, nämlich die Vertraulichkeit von Kommunikationsumständen.[245]
- Die Schutzziele stehen darüber hinaus auch zueinander im Widerspruch: So steht etwa die Forderung von Anonymität in diametralem Gegensatz zu der ebenso erhobenen Forderung nach Zurechenbarkeit. Vertraulichkeit verlangt das Gegenteil von Verfügbarkeit.[246]

Insoweit ist fraglich, ob eine Abgrenzung von Schutzzielen überhaupt möglich ist.[247] In der Literatur findet sich sogar die Aussage, dass es „praktisch ausgeschlos-

239 *Hammer*, Die 2. Dimension der IT-Sicherheit, S. 141.
240 Vgl. *Federrath/Pfitzmann*, IT-Sicherheit, in: *Wind/Kröger,* Handbuch IT in der Verwaltung, S. 273, 273.
241 So auch *Schneier*, Secrets and Lies, S. 122.
242 Etwa von *Eckert*, IT-Sicherheit, S. 6 f.
243 Siehe auch Dierstein, IT-Sicherheit und ihre Besonderheiten – Duale Sicherheit –, verfügbar unter: http://www.bayer.in.tum.de/lehre/WS2003/ITS-dierstein/DualSi.pdf (28.01.2008), S. 13; *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 221.
244 So *Raepple*, Sicherheitskonzepte für das Internet, S. 5 ff.
245 Neben „Anonymität" kann auch „Unbeobachtbarkeit" als Teilgewährleistungen von „Vertraulichkeit" verstanden werden; vgl. *Federrath/Pfitzmann*, IT-Sicherheit, in: *Wind/Kröger,* Handbuch IT in der Verwaltung, S. 273, 274.
246 *Federrath/Pfitzmann,* DuD 2000, 704, 710.
247 In der Praxis wird daher häufig mit Gefährdungs- und Maßnahmekatalogen (etwa die IT-Grundschutz-Kataloge des BSI, die das IT-Grundschutzhandbuch ersetzen, verfügbar unter http://www.bsi.de/gshb/deutsch/index.htm (19.02.2008)) und weniger mit abstrakten Schutzzielen gearbeitet; vgl. auch *Hammer*, Die 2. Dimension der IT-Sicherheit, S. 139 ff.

sen [sei; d. Verf.], ein IT-Sicherheitsziel zu verletzen, ohne auch die anderen Schutzziele zu beeinträchtigen“[248]:

> „So sind etwa Integrität, Verfügbarkeit und Zurechenbarkeit von Daten nicht mehr gewährleistet, wenn die Vertraulichkeit bestimmter Informationen (z.B. der Passwörter) kompromittiert ist. Die Schutzziele Vertraulichkeit, Verfügbarkeit und Zurechenbarkeit sind wiederum abhängig von dem Sicherheitsziel der Integrität, wenn z.B. ein Passwort unbemerkt geändert worden ist.“[249]

Angesichts der selbst innerhalb der Informatik noch nicht geklärten terminologischen und definitorischen Fragen kann hier nur eine Darstellung der verschiedenen Ansätze zur Kategorisierung und Definition von Schutzzielen versucht werden:

aa) Schutzziel-Trias: Vertraulichkeit, Integrität, Verfügbarkeit

Klassischerweise[250] wurde eine Trias von Schutzzielen unterschieden, nämlich

- Vertraulichkeit (`*confidentiality´*),
- Integrität (`*integrity´*) und
- Verfügbarkeit (`*availability´*).

Nach dem europäischen Standard der `*Information Technology Security Evaluation Criteria´* (ITSEC[251]) werden die drei Schutzziele wie folgt definiert:

> „Vertraulichkeit – Schutz vor unbefugter Preisgabe von Informationen;
>
> - Integrität – Schutz vor unbefugter Veränderung von Informationen;
>
> - Verfügbarkeit – Schutz vor unbefugter Vorenthaltung von Informationen oder Betriebsmitteln.“[252]

Soweit sonstige Definitionen dieser Schutzziele zu finden sind, sind diese im Wortlaut ähnlich und scheinen jedenfalls im Kern übereinzustimmen.[253] Hinsichtlich dieses klassischen Kernbestands an Schutzzielen scheint weit reichende Einigkeit zu herrschen.

248 *Holznagel*, Recht der IT-Sicherheit, S. 15.
249 *Holznagel*, Recht der IT-Sicherheit, S. 15.
250 So etwa Bundesamt für Sicherheit in der Informationstechnik, IT-Sicherheitshandbuch, verfügbar unter: http://www.bsi.de/literat/kriterie.htm (13.02.2008), Kap. 3.1; *Schneier*, Secrets and Lies, S. 121; *Federrath/Pfitzmann*, IT-Sicherheit, in: *Wind/Kröger,* Handbuch IT in der Verwaltung, S. 273, 273.
251 Verfügbar unter http://www.bsi.de/zertifiz/itkrit/itsec.htm (13.02.2008); siehe dazu auch *Holznagel*, Recht der IT-Sicherheit, S. 39 f.
252 Ziffer 0.2 Information Technology Security Evaluation Criteria (ITSEC); http://www.bsi.de/zertifiz/itkrit/itse c-dt.pdf (13.02.2008).
253 Vgl. etwa die Definitionen von *Eckert*, IT-Sicherheit, S. 7 ff.; *Federrath/Pfitzmann*, IT-Sicherheit, in: *Wind/ Kröger,* Handbuch IT in der Verwaltung, S. 273, 273; *Raepple*, Sicherheitskonzepte für das Internet, S. 4; *Holznagel*, Recht der IT-Sicherheit, S. 12.

bb) Authentizität

Es gibt darüber hinaus vielfältige Vorschläge, den Katalog der drei klassischen Schutzziele um zusätzliche Schutzziele zu erweitern:[254] *Eckert* nennt etwa als weiteres Schutzziel die Authentizität (`*authenticity*´), welche als

> „die Echtheit und Glaubwürdigkeit des Objekts bzw. Subjekts, die anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar ist“[255]

definiert wird. Hier wird Authentizität als Teilaspekt der Integrität verstanden (s.o. unter II.1.):[256] Die unbefugte Veränderung von Daten (Schutz der Integrität) kann nur verhindert werden, wenn feststellbar ist, welche Subjekte befugt oder unbefugt sind (Authentizität).[257]

Im Gegensatz dazu umfassen zwar – zumindest nach der Definition nach ITSEC – auch die Schutzziele der Vertraulichkeit und Verfügbarkeit Authentizitätsaspekte, die Feststellung der Unbefugtheit ist aber nicht im gleichen Maße konstitutiv für das Vorliegen einer Schutzzielverletzung wie im Rahmen des Schutzziels Integrität: Bei (nahezu) jeder Aktion werden die Daten zugleich auch verändert. So werden etwa beim Routen von Datenpaketen diese Datenpakete verändert (der Header wird jeweils um den durchlaufenen Router ergänzt). Der `Unbefugtheit´ der Datenveränderung kommt daher zentrale Bedeutung bei der Identifizierung von Integritätsverletzungen zu. Der Verweis auf die `Unbefugtheit´ der Datenpreisgabe bzw. –vorenthaltung im Rahmen der Vertraulichkeit und Verfügbarkeit hat dagegen eher klarstellenden Charakter. Der Schwerpunkt der Authentizitätsfragen liegt im Bereich der Integrität, was die hier vorgenommene Zuordnung rechtfertigt.[258] Ein gesondertes Schutzziel `Authentizität´ ist daneben nicht erforderlich.

254 Vgl. *Raepple*, Sicherheitskonzepte für das Internet, S. 4 ff.; *Federrath/Pfitzmann*, IT-Sicherheit, in: *Wind/ Kröger,* Handbuch IT in der Verwaltung, S. 273, 273 ff.; *Eckert*, IT-Sicherheit, S. 7 ff.; *Federrath/Pfitzmann,* DuD 2000, 704, 705 f.

255 *Eckert*, IT-Sicherheit, S. 6.

256 Siehe auch Dierstein, IT-Sicherheit und ihre Besonderheiten – Duale Sicherheit –, verfügbar unter: http://www.bayer.in.tum.de/lehre/WS2003/ITS-dierstein/DualSi.pdf (28.01.2008), S. 13; *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 221.

257 Hier geht es um eine rein (informations-)technische Kategorisierung von Schutzzielen. In einer (zivil-)rechtlichen Perspektive kann die Unterscheidung von Authentizitätsverletzungen (etwa Handeln unter fremdem Namen) und Integritätsverletzungen durchaus bedeutsam sein. Hier kommt es darauf aber nicht an.

258 Im Bereich der Vertraulichkeit ergibt sich die Befugnis häufig schon aus der Eigenschaft als Sender oder Empfänger in einer Kommunikationsbeziehung. Im Rahmen der Verfügbarkeit liegt der Schwerpunkt stärker auf dem Schutz vor Vorenthaltung als dem Schutz vor *unbefugter* Vorenthaltung.

cc) Verbindlichkeit, Zurechenbarkeit, Revisionsfähigkeit/Rechtsverbindlichkeit

Als weiteres Schutzziel nennt *Eckert* Verbindlichkeit (*`non repudiation´*), die gewährleistet sein soll,

> „wenn es nicht möglich ist, dass ein Subjekt im Nachhinein die Durchführung einer solchen Aktion abstreiten kann.“[259]

Dies dürfte in der Sache mit den vorgeschlagenen Schutzzielen der Zurechenbarkeit (*`accountability´*)

> „Von jeder in einem IT-System ausgeführten Aktion (Vorgang, Prozess) muss während ihres Ablaufs und danach feststellbar sein, wem, d.h. welcher Instanz – insbesondere welcher Person – diese Aktion zuzuordnen ist, welches Subjekt sie ausgelöst und wer sie letztlich zu *verantworten* hat.“[260]

und der Revisionsfähigkeit/Rechtsverbindlichkeit (*`legal liability´*)

> „Beim rechtsverbindlichen Einsatz der Informationstechnik in der Praxis […] muss den in einem IT-System (Netz) ablaufenden Aktionen (Vorgängen, Prozessen) und den aus ihnen gewonnenen Ergebnissen hinreichend verlässlich *Beweiskraft* zugemessen werden können. Insbesondere muss für jeden Vorgang und dessen Ergebnisse zweifelsfrei *auch für Dritte erkennbar und beweisbar* sein, welcher auslösenden Instanz die Verantwortung für Ergebnisse und Folgen einer Aktion zuzurechnen ist.“[261]

übereinstimmen. Welcher Terminologie und Definition man auch den Vorzug geben mag, ist ihnen gemeinsam, dass die Schutzziele Verbindlichkeit, Zurechenbarkeit wie Revisionsfähigkeit/Rechtsverbindlichkeit allesamt der Festschreibung gesellschaftlicher Anforderungen an Informationstechnologie dienen.[262] *Dierstein* hat diese Dimension von IT-Sicherheit daher mit Beherrschbarkeit (*`controllability´*) überschrieben, die er wie folgt definiert:

> „Sachlage, bei der Rechte oder schutzwürdige Belange der Betroffenen durch das Vorhandensein oder die Nutzung von IT-Systemen nicht unzulässig beeinträchtigt werden.“[263]

Dabei hat er deutlich herausgearbeitet, dass es sich gerade *nicht um Anforderungen der technischen Sicherheit des Systems* handelt (darunter fasst auch *Dierstein* nur Vertraulichkeit, Verfügbarkeit und Integrität und überschreibt diesen Bereich insgesamt mit dem Begriff der Verlässlichkeit; *`dependability´*), sondern um die *Sicherheit der Betroffenen vor dem System*.[264]

Im Rahmen dieser Arbeit geht es um eine rein technische Betrachtung der IT-Sicherheit des Systems. Gesellschaftliche Anforderungen im Sinne einer Sicherheit vor dem System bleiben außer Betracht, so dass hier Verbindlichkeit, Zurechenbarkeit und Revisionsfähigkeit/Rechtsverbindlichkeit keine relevanten Schutzziele sind.

259 *Eckert*, IT-Sicherheit, S. 11.
260 *Dierstein,* InfSpekt 2004, 343, 349.
261 *Dierstein,* InfSpekt 2004, 343, 349.
262 *Dierstein,* InfSpekt 2004, 343, 346 ff.
263 *Dierstein,* InfSpekt 2004, 343, 346.
264 *Dierstein,* InfSpekt 2004, 343, 346.

dd) Anonymität

Ohne klarzustellen, ob es sich um ein weiteres Schutzziel handeln soll, wird daneben auch die Gewährleistung der Anonymität von Subjekten als Forderung genannt.[265] Anonymität wird danach erreicht durch Anonymisierung, d.h.

> „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können"[266]

und Pseudomisierung, d.h.

> „das Verändern personenbezogener Daten durch eine Zuordnungsvorschrift (z.B. die Verwendung von Pseudonymen) derart, dass Einzelangaben über persönliche oder sachliche Verhältnisse ohne Kenntnis der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können."[267]

Pseudomisierung ist also sowohl in einer technischen wie in einer rechtlichen Perspektive kein eigenständiges Schutzziel, sondern ein Mittel zur (weitgehenden[268]) Erreichung von Anonymität. Anonymität ist aber ebenfalls kein eigenständiges Schutzziel, sondern ein Aspekt von Vertraulichkeit – die Vertraulichkeit von Kommunikationsumständen (s.o. unter I.1.c.).[269]

ee) Ergebnis

Da die Vorschläge zur Anerkennung weiterer, über die drei klassischen hinausgehenden Schutzziele nicht überzeugen können, soll hier allein auf die hergebrachte Schutzziel-Trias zurückgegriffen werden.[270] Diese Schutzziele finden zum einen breite Anerkennung und decken zum anderen bei weiter Auslegung durchaus alle

265 *Eckert*, IT-Sicherheit, S. 12.

266 *Eckert*, IT-Sicherheit, S. 12; so auch die Definition in § 3 VI BDSG: „Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können."

267 *Eckert*, IT-Sicherheit, S. 12; die Definition in § 3 VIa BDSG lautet abweichend davon: „Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren."

268 Die Anonymität ist gerade nicht vollständig, da eine Zuordnungsvorschrift existiert – diese ist aber nur eingeschränkt bekannt.

269 So auch *Federrath/Pfitzmann*, IT-Sicherheit, in: *Wind/Kröger,* Handbuch IT in der Verwaltung, S. 273, 274.

270 Dies entspricht auch dem Ansatz von *Hansen/Pfitzmann*, Techniken der Online-Durchsuchung: Gebrauch, Missbrauch, Empfehlungen, in: *Roggan,* Online-Durchsuchungen, S. 131, 132.

grundlegenden Aspekte von IT-Sicherheit ab – wenn man etwa der pointierten Definition von *B. Schneier* folgt:

Danach entspricht Vertraulichkeit dem Schutz vor unbefugtem Lesen von Daten und Integrität dem Schutz vor unbefugtem Schreiben von Daten.

> „This definition of integrity illustrates how closely it is related to confidentiality. The latter is about unauthorized reading of data (and programs); the former is about unauthorized writing."[271]

Verfügbarkeit definiert *Schneier* wie folgt:

> „We want the computer to work when we expect it to as we expect it to."[272]

Teilweise wurden die Schutzziele sogar noch weiter auf lediglich zwei Ziele reduziert: Vertraulichkeit und totale Korrektheit.[273] Allerdings steht dieser Ansatz unter der Voraussetzung, dass alle (legalen) Anfragen an das System auch befriedigt werden können. Dies ist letztlich ein Gedanke der Verfügbarkeit. Es bleibt daher bei der hergebrachten Konturierung des Begriffs der IT-Sicherheit durch die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit.

b. `*Safety*´ und `*security*´

Neben den Schutzzielkatalogen ist auch immer wieder die Unterscheidung von `*safety*´ und `*security*´ zu finden.[274] `*Safety*´ wird teilweise mit Funktionssicherheit eines Systems übersetzt, `*security*´ mit Informationssicherheit:[275]

> „ Unter Funktionssicherheit (engl. *safety*) eines Systems verstehen wir die Eigenschaft, dass die realisierte Ist-Funktionalität der Komponenten mit der spezifizierten Soll-Funktionalität übereinstimmt. Ein funktionssicheres System nimmt keine funktional unzulässigen Zustände an. Anders formuliert verstehen wir unter der Funktionssicherheit eines Systems, dass es unter allen (normalen) Betriebsbedingungen funktioniert. Die Informationssicherheit (engl. *security*) ist die Eigenschaft eines funktionierenden Systems, nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder –gewinnung führen."[276]

`*Safety*´ adressiert im Wesentlichen solche Bedrohungen, die durch das technische Fehlverhalten des Systems selbst, also *von innen*, entstehen, z.B. durch Programmierfehler.[277] IT-Sicherheit beschäftigt sich dagegen schwerpunktmäßig mit

271 *Schneier*, Secrets and Lies, S. 122.
272 *Schneier*, Secrets and Lies, S. 122.
273 *Federrath/Pfitzmann,* DuD 2000, 704, 706.
274 *Eckert*, IT-Sicherheit, S. 4 f.; *Schmeh*, Kryptografie und Public-Key-Infrastrukturen im Internet, S. 14 f.
275 *Eckert*, IT-Sicherheit, S. 4 f.
276 *Eckert*, IT-Sicherheit, S. 4 f.
277 *Eckert*, IT-Sicherheit, S. 6; ähnlich auch RFC 4949: Internet Security Glossary, Version 2 vom August 2007, verfügbar unter http://www.heise.de/netze/rfc/rfcs/rfc4949.shtml (29.05. 2009), S. 257: „safety – The property of a system being free from risk of causing harm (especially physical harm) to its system entities."

Bedrohungen *von außen*, also mit Fragen der `*security*´. Teilweise werden `*security*´ und `*safety*´ danach unterschieden, ob es sich um beabsichtigte (`*security*´) oder unbeabsichtigte (`*safety*´) Sicherheitsbedrohungen handelt.[278]

Diese abweichenden Ansätze verdeutlichen schon, dass auch hier wenig terminologische Klarheit und definitorische Einigkeit herrscht.[279] Für eine klarere Abgrenzung des Begriffs der IT-Sicherheit scheinen die Termini `*safety*´ und `*security*´ daher wenig hilfreich zu sein. Daneben sprechen weitere Argumente gegen die Verwendung des Begriffspaares `*safety*´ – `*security*´ zur Definition von IT-Sicherheit: für die Vertrauenswürdigkeit eines Systems ist es letztlich zweitrangig, ob eine Fehlfunktion absichtlich oder unabsichtlich herbeigeführt wurde.[280] Die Grenze zwischen Fragen der `*safety*´ und solchen der `*security*´ verschwimmt in diesem Bereich und die Kategorien überlappen sich teilweise.[281] Schließlich adressiert IT-Sicherheit schwerpunktmäßig Bedrohungen durch absichtliche Manipulation, mithin Fragen der `*security*´. Die Einteilung in `*safety*´ und `*security*´ ist daher für eine Definition von IT-Sicherheit nicht weiterführend und verliert darüber hinaus allgemein in der Informationstechnik an Bedeutung.[282]

Im Rahmen der hier dargestellten rein technisch bedingten IT-Sicherheitsanforderungen bleibt es daher bei der dargestellten Annäherung an den IT-Sicherheitsbegriff über die Schutzziel-Trias Vertraulichkeit, Integrität und Verfügbarkeit.

2. Verschlüsselung zur Gewährleistung von IT-Sicherheit

Zur Gewährleistung dieser Schutzziele sind nach dem Stand der Technik Verschlüsselungsverfahren essentiell:

- Verschlüsselungsverfahren sind zum einen essentiell für die Gewährleistung der *Vertraulichkeit* von Kommunikationsinhalten wie –umständen. Alternativen zu Verschlüsselungsverfahren, die über einen ähnlichen, hohen Sicherheitsstandard verfügen und die notwendige Praktikabilität als Massenanwendung aufweisen, existieren derzeit nicht.[283]
- Verschlüsselungsverfahren sind nach dem derzeitigen Stand der Technik ebenso essentiell für die Gewährleistung der *Integrität*. In so genannten `sicheren´ Umgebungen erfordert der Integritätsschutz eine wirksame und sichere Rechteverwaltung. Die (IT-)Sicherheit dieser Rechteverwaltung ist durch Verschlüsselungsverfahren zu gewährleisten. Da sich die Integrität auf den Schutz vor *unbefugter* Veränderung von Informationen bezieht, kommt der zuverlässigen Fest-

278 *Federrath/Pfitzmann,* DuD 2000, 704, 704; *Dierstein,* InfSpekt 2004, 343, 343 f.
279 *Dierstein,* InfSpekt 2004, 343, 343.
280 *Dierstein,* InfSpekt 2004, 343, 344.
281 *Eckert*, IT-Sicherheit, S. 6; *Laprie*, Dependability of Computer Systems: from Concepts to Limits, IFIP International Workshop on Dependable Computing and its Applications (DCIA´98), Johannesburg, 12.-14. Januar 1998, S. 108, 108 f.
282 *Dierstein,* InfSpekt 2004, 343, 343 f.
283 Siehe oben unter I.3. und 4.

stellung der Identität eines Nutzers – neben der sicheren Zuordnung seiner individuellen Berechtigungen – zentrale Bedeutung zu. Die Authentizität als Teilaspekt der Integrität erfordert in der derzeitigen Praxis sehr häufig (aber nicht zwingend!) ebenfalls die Verwendung von Verschlüsselungsverfahren.[284] In so genannten `unsicheren´ Umgebungen fordert der Integritätsschutz, dass unbefugte Veränderungen erkennbar sein müssen. Dies wird durch den Einsatz von Hashverfahren und `*Message Authentication Codes´* umgesetzt. Beide basieren auf Verschlüsselungsverfahren. Alternativen zum Einsatz von Verschlüsselungsverfahren sind derzeit nicht ersichtlich.[285]

- Lediglich das Schutzziel *Verfügbarkeit* wird regelmäßig nicht bzw. nicht vollständig durch den Einsatz von Verschlüsselungsverfahren gewährleistet.[286] Mit dem Trend weg vom klassischen zentralisierten Rechenzentrum und hin zu verteilten Systemen haben sich allerdings auch die Schwerpunkte der Anforderungen an IT-Sicherheit verschoben: Während bei zentralisierten Rechenzentren Fragen der Verfügbarkeit (Ausfallsicherheit, Fehlertoleranz etc.) eine tragende Rolle spielten, rückt bei verteilten Systemen der Schutz vor Verfälschung, Manipulation und unbefugtem Mitlesen – also: der Schutz von Integrität und Vertraulichkeit – in den Vordergrund.[287]

Die entscheidenden Anforderungen der IT-Sicherheit werden mithin durch Verschlüsselungsverfahren gewährleistet. Verschlüsselung wurde daher zu Recht als eine Kerntechnologie des Cyberspace bezeichnet:

> „[C]ryptography is a core technology of cyberspace. It lets us take all of the business and social constructs we´re used to in the physical world, and move them to cyberspace. It´s the technology that let us build security into cyberspace […].“[288]

Verschlüsselung ist in einer technischen Betrachtungsweise die IT-Sicherheitstechnologie weltweiter Computernetze.[289]

284 Nur die eigenschaftsbasierte Authentifikation bedarf keines Einsatzes von Verschlüsselungsverfahren (s.o.). In der praktischen Anwendung ist aber die wissensbasierte Authentifikation am häufigsten anzutreffen; *Eckert*, IT-Sicherheit, S. 432.

285 Siehe oben unter II.3.

286 BSI: E-Government-Handbuch; „Verschlüsselung und Signatur – Grundlagen und Anwendungsaspekte“, verfügbar unter: http://www.bsi.de/fachthem/egov/download/2_Krypto.pdf (26.02.2008), S. 14.

287 *Federrath/Pfitzmann,* DuD 2000, 704, 704. Siehe ausführlich zu den veränderten Anforderungen des sog. `Cloud Computing´ ENISA, Cloud Computing – Benefits, Risks and Recommendations for Information Security, verfügbar unter: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReportta (23.11.2009).

288 *Schneier*, Secrets and Lies, S. 85.

289 Vgl. *Buchmann*, Einführung in die Kryptographie, im Vorwort. So auch TAUCIS, Technikfolgenabschätzungsstudie Ubiquitäres Computing, verfügbar unter: http://www.taucis.hu-berlin.de/_download/TAUCIS_Studie.pdf (25.09.2008), S. 252: „Kryptographie (z.B. kryptographische Hashfunktionen, symmetrische Verschlüsselungsverfahren wie AES oder asymmetrische wie RSA) ist das Hauptwerkzeug, um Informationssicherheit sicherzustellen […]“.

C. Bedeutung von Verschlüsselung – eine einfachgesetzliche Perspektive

I. Einfachgesetzliche Definition von Verschlüsselung

Eine einfachgesetzliche Definition von Verschlüsselung findet sich – soweit ersichtlich – nur in § 3a IV lit. c Berliner Datenschutzgesetz:[290]

> „(4) Im Sinne dieses Gesetzes ist […] c) Verschlüsselung das Ersetzen von Klartextbegriffen oder Zeichen durch andere in der Weise, dass der Klartext nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wieder lesbar gemacht werden kann."

Diese Definition scheint allerdings nur die Gewährleistung der Vertraulichkeit durch Verschlüsselung zu umfassen. Die einzige Verschlüsselungsvorschrift, die das Berliner Datenschutzgesetz enthält, betrifft den Schutz der Vertraulichkeit bei Datenübermittlungen; vgl. § 3a II S. 2, Nr. 9 Berliner Datenschutzgesetz:

> „(2) Eine Wartung durch andere Stellen darf über die Anforderungen nach Absatz 1 hinaus nur auf Grund schriftlicher Vereinbarungen erfolgen. Darin sind folgende Regelungen zu treffen: […] 9. Verschlüsselung von personenbezogenen Daten auf dem Übertragungsweg nach dem jeweiligen Stand der Technik […]."

II. Einfachgesetzliche Verschlüsselungspflichten

1. Explizite Verschlüsselungspflichten bei Datenübermittlungen (grammatische Auslegung)

Zunächst kann festgestellt werden, dass zahlreiche einfachgesetzliche Normen ausdrückliche Verschlüsselungspflichten für Datenübermittlungen, insbesondere via Internet, vorsehen:

- Es sind einige einfachgesetzliche Normen zu finden, die den Einsatz von Verschlüsselungsverfahren im Fall der Nutzung allgemein zugänglicher Netze ausdrücklich vorschreiben;[291] vergleiche etwa § 11 II WpAIV:[292]

  > „Die Bundesanstalt kann die Möglichkeit eröffnen, die Mitteilungen nach § 15a des Wertpapierhandelsgesetzes im Wege der Datenfernübertragung zu übersenden, sofern dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit getroffen werden, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten

290 Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung i.d.F. vom 17.12. 1990 (GVBl.1991 S. 16).

291 Sei es, dass sich diese Normen an die staatliche Stelle richten wie beim folgenden Beispiel § 11 II WpAIV, sei es, dass der Grundrechtsberechtigte selbst dazu verpflichtet wird wie bei § 4 III S. 11 FPersG.

292 Verordnung zur Konkretisierung von Anzeige-, Mitteilungs- und Veröffentlichungspflichten sowie der Pflicht zur Führung von Insiderverzeichnissen nach dem Wertpapierhandelsgesetz (Wertpapierhandelsanzeige- und Insiderverzeichnisverordnung – WpAIV) vom 13.12.2004 (BGBl. I S. 3376).

gewährleisten, und sofern im Fall der Nutzung allgemein zugänglicher Netze dem jeweiligen Stand der Technik entsprechende Verschlüsselungsverfahren angewendet werden."[293]

Das Internet ist dabei sicherlich das Paradebeispiel für ein „allgemein zugängliches Netz".

- Im hessischen Landesrecht wird zum Teil auch ausdrücklich auf Datenübermittlungen via Internet Bezug genommen; vergleiche etwa § 17 I S. 2 und 3 Hessisches Meldegesetz:

  „Hat die Meldebehörde für die Anmeldung einen Internet-Zugang eröffnet, können sich Meldepflichtige durch die Übermittlung der angeforderten Angaben unter Verwendung einer qualifizierten elektronischen Signatur nach dem Signaturgesetz über diesen Zugang anmelden. Der Zugang muss eine dem Stand der Technik entsprechende Verschlüsselung der übermittelten Daten sicherstellen."[294]

- Teilweise impliziert auch der Kontext einer Verschlüsselungspflicht, dass es sich um Datenübermittlungen über Internet handeln muss; vergleiche etwa § 87a I S. 3 AO:

  „(1) Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet. Ein elektronisches Dokument ist zugegangen, sobald die für den Empfang bestimmte Einrichtung es in für den Empfänger bearbeitbarer Weise aufgezeichnet hat. Übermittelt die Finanzbehörde Daten, die dem Steuergeheimnis unterliegen, sind diese Daten mit einem geeigneten Verfahren zu verschlüsseln."[295]

- Teilweise ist ausdrücklich für jeden Fall der Datenübermittlung eine Verschlüsselung vorgeschrieben, unabhängig davon, ob es sich um öffentliche Netze oder verwaltungsinterne Intranets handelt; vergleiche etwa § 28a I SGB IV:

  „Der Arbeitgeber oder ein anderer Meldepflichtiger hat der Einzugsstelle für jeden in der Kranken-, Pflege-, Rentenversicherung oder nach dem Recht der Arbeitsförderung kraft Gesetzes Versicherten […] eine Meldung durch gesicherte und verschlüsselte Datenübertragung aus systemgeprüften Programmen oder mittels maschinell erstellter Ausfüllhilfen zu erstatten."[296]

- Vereinzelte Vorschriften enthalten nur eine Verschlüsselungs*option*, schreiben eine Verschlüsselung also nicht bindend vor, wobei staatliche Behörden ihr diesbezügliches Ermessen korrekt ausüben müssen; so etwa § 23 S. 1 TEHG:

293 Vgl. auch §§ 28a XIII S. 3; 101 I S. 3 und 103 IV S. 2 SGB IV; § 4 III S. 12, 2. Hs. FPersG; § 1 III 2. Hs. Verordnung über die elektronische Übermittlung von für das Besteuerungsverfahren erforderlichen Daten (Steuerdaten-Übermittlungsverordnung); § 2 II S. 2, 2. Hs. Verordnung über das Zentrale Vorsorgeregister; § 2 VI S. 2, 2. Hs. Verordnung zur Durchführung des Fahrpersonalgesetzes (Fahrpersonalverordnung); § 12 I S. 3, 2. Hs. des Entwurfs eines Gesetzes über Personalausweise und den elektronischen Identitätsnachweis vom 07.10.2008, BT-Drs. 16/10489.

294 Ähnlich auch § 9 II S. 2 Hess. MeldeG.

295 So sprechen etwa § 16b Nr. 1 II S. 3 und § 21 Nr. 1 II S. 3 VOL/A – Bestimmungen nach der EG-Sektorenrichtlinie sowie § 8 Nr. 3, S. 3 VOL/A-SKR von „elektronisch übermittelten" Angeboten und Teilnahmeanträgen.

296 Parallele Anforderungen an die Datenübertragung stellen auch §§ 23c II S. 2; 28a X, S. 2; 101 I S. 4 SGB IV. Eine ausdrückliche Verschlüsselungspflicht enthält auch § 17 Ia, S. 2 Hessische Beihilfenverordnung.

„Die zuständige Behörde kann für die Bekanntgabe von Entscheidungen und die sonstige Kommunikation die Verwendung der elektronischen Form, eine bestimmte Verschlüsselung sowie die Eröffnung eines Zugangs für die Übermittlung elektronischer Dokumente vorschreiben."

Angesichts der Vertraulichkeitsgefahren bei Datenübermittlungen via Internet spricht viel dafür, dass die zuständige Behörde bei elektronischer Kommunikation via Internet im Wege einer Ermessensreduktion auf Null[297] die Verwendung von Verschlüsselung vorschreiben muss. Die Ermessenseinräumung bezieht sich demnach allein auf die Frage, ob eine *bestimmte* Verschlüsselung vorgeschrieben wird, und nicht darauf, ob überhaupt Verschlüsselung verlangt wird.

2. Verschlüsselung zum „Schutz gegen unbefugte Kenntnisnahme" bei Datenübermittlungen (teleologische Auslegung)

Daneben sehen viele Normen den Schutz „gegen unbefugte Kenntnisnahme",[298] den Schutz der „Vertraulichkeit"[299] oder auch den Schutz davor, dass Daten bei der Übermittlung „unbefugt gelesen"[300] werden können, vor. Schutz gegen unbefugte Kenntnisnahme wie auch Schutz davor, dass Daten nicht unbefugt gelesen werden, bedeuten dabei in teleologischer Auslegung nichts anderes als Schutz der Vertraulichkeit von Kommunikationsinhalten.[301]

Zu prüfen ist, welche konkreten Maßnahmen zur Gewährleistung der Vertraulichkeit erforderlich sind, und vor allem, ob und wann sich aus den Vertraulichkeitsanforderungen (zwingend) der Einsatz von Verschlüsselungsverfahren ergibt. Verschlüsselung ist nach dem Stand der Technik *das* Verfahren zur Gewährleistung der Vertraulichkeit von Kommunikationsinhalten. Entscheidend ist daher, welches

297 Siehe dazu unten in Teil 6 unter A.I.5.b.cc).

298 Vgl. etwa § 78 II S. 5 FGO: „Für die Übermittlung von elektronischen Dokumenten ist die Gesamtheit der Dokumente mit einer qualifizierten elektronischen Signatur nach § 2 Nr. 3 des Signaturgesetzes zu versehen und gegen unbefugte Kenntnisnahme zu schützen."; so oder ähnlich auch § 140 II S. 3 GBO; § 110d II S. 2, 2. Hs. OWiG; § 120 II S. 5 SGG; § 38 V S. 1 StVG; § 100 II S. 5 VwGO; § 174 III S. 3 und § 299 III S. 4 ZPO. § 20k II S. 3 BKAG verlangt den Schutz der im Rahmen der Online-Durchsuchung kopierten Daten „gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme".

299 Etwa § 24c VI S. 1 KWG: „Das Kreditinstitut und die Bundesanstalt haben dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der abgerufenen und weiter übermittelten Daten gewährleisten."

300 Vgl. etwa Nr. 9 der Anlage zu § 126 I S. 2 Nr. 3 GBO: „Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind, […] zu verhindern, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle), […]"; ähnlich auch Nr. 4 der Anlage zu § 78a SGB X.

301 Vgl. nochmals die Definition nach ITSEC: „Vertraulichkeit –Schutz vor unbefugter Preisgabe von Informationen".

Schutzniveau der Gesetzgeber vorschreibt. Ist ein möglichst hohes Schutzniveau erforderlich oder reichen irgendwelche den Vertraulichkeitsschutz fördernden Maßnahmen aus? Da der Gesetzgeber in den hier diskutierten Fällen gerade nicht ausdrücklich den Einsatz von Verschlüsselung vorgeschrieben hat, ergibt sich folgendes: Zum einen ist der Ansatz, nur ein Schutzziel vorzugeben, die konkrete technische Umsetzung aber offen zu lassen, als pragmatisch anzusehen, da die Norm so flexibel ist hinsichtlich technologischer Veränderungen und technischen Fortschritts. Zum zweiten dürfte daraus geschlossen werden können, dass der Gesetzgeber auch im Übrigen eine flexible Handhabung der Vorschrift nach den tatsächlichen Gegebenheiten im Einzelfall ermöglichen wollte. Die konkrete Risikoanalyse spielt dabei eine herausgehobene Rolle.

a. „Schutz gegen unbefugte Kenntnisnahme“ in unsicheren Umgebungen, insbesondere allgemein zugänglichen Netzen

So sind Daten, die in allgemein zugänglichen Netzen übermittelt werden, qualitativ und quantitativ völlig andersartigen Bedrohungen ausgesetzt als Daten, die auf nicht mit dem Internet verbundenen Rechnern in nur bestimmten Personen zugänglichen Räumen gespeichert sind. Für den letzteren Fall könnte ein sonstiges Sicherheitskonzept ohne den Einsatz von Verschlüsselungsverfahren ausreichend sein. Für die erste Variante ist dagegen der Einsatz von Verschlüsselungsverfahren – angesichts der grundsätzlich für jedermann bestehenden Kenntnisnahmemöglichkeit bei Datenübermittlung im Internet – unerlässlich. *Daher ergibt sich aus gesetzlichen Normen, die den Schutz der Vertraulichkeit, den Schutz vor unbefugter Kenntnisnahme usw. vorschreiben, eine Verschlüsselungspflicht.* Dieses Ergebnis wird etwa durch § 4 III S. 12 FPersG bestätigt:

> „Im Falle der Datenfernübertragung sind dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit, Unversehrtheit und Zurechenbarkeit der Daten gewährleisten; im Falle der Nutzung allgemein zugänglicher Netze sind dem jeweiligen Stand der Technik entsprechende Verschlüsselungsverfahren anzuwenden.“[302]

302 So oder mit fast identischem Wortlaut auch § 89a VIII AufenthG; § 20 k II, S. 3 BKAG; § 78a II S. 2 BNotO; § 16a VI S. 1 GenTG; § 17 II S. 2 SchwarzArbG; §§ 488 I S. 2 und 493 I S. 2 StPO; § 30a II Nr. 1 StVG; § 36 V Nr. 2 StVG; § 53 II Nr. 1 StVG; § 6 Verordnung über das datenbankgestützte Informationssystem über Medizinprodukte des Deutschen Instituts für Medizinische Dokumentation und Information; § 4 I S. 1 und 2 Verordnung zur Durchführung der steuerlichen Vorschriften des Einkommensteuergesetzes zur Altersvorsorge; § 28 VI S. 3 Verordnung über den Schutz vor Schäden durch Röntgenstrahlen; § 5 III Verordnung über die Anzeige von Versicherungsfällen in der gesetzlichen Unfallversicherung (Unfallversicherungs-Anzeigeverordnung); § 16 S. 2 und 3 Verordnung über die Erfassung und Übermittlung von Daten für die Träger der Sozialversicherung (Datenerfassungs- und –übermittlungsverordnung); § 6 I S. 2 Verordnung über Meldungen internationaler Adoptionsvermittlungsfälle an die Bundeszentralstelle für Auslandsadoption (Auslandsadoptions-

In dieser Norm – sowie in etlichen Normen mit parallelem Wortlaut – wird aus der generellen Verpflichtung zur Gewährleistung der Vertraulichkeit eine qualifizierte Verpflichtung zum Einsatz von Verschlüsselung bei Nutzung allgemein zugänglicher Netze. Es handelt sich um einen Sonderfall der Gewährleistung von Vertraulichkeit. Die Norm verdeutlicht die gesetzgeberische Wertung, dass die Vertraulichkeitsgefahren bei Datenübermittlung im Internet so gewichtig sind, dass nur Verschlüsselungsverfahren das Vertraulichkeitsgebot adäquat umsetzen können. *Auch wenn andere Normen dies nicht explizit so normiert haben, enthält doch das allgemeine Vertraulichkeitsgebot für bestimmte Fälle eine Pflicht zum Einsatz von Verschlüsselung. Nämlich dann, wenn staatliche Stellen nicht ermessensfehlerfrei andere Sicherheitsmaßnahmen zur Vertraulichkeitsgewährleistung einsetzen könnten (Ermessensreduktion auf Null). Die soeben genannten Normen zeigen, dass die Datenübermittlung via Internet so ein Fall ist*: Angesichts der Bedeutung privater Daten einerseits und der Sicherheitsbedrohungen bei der Übermittlung andererseits, ist angemessener Vertraulichkeitsschutz nach derzeitigem Stand der Technik nur durch den Einsatz von Verschlüsselungsverfahren möglich. Eine solche Auslegung kommt aber nur da in Betracht, wo überhaupt einfachgesetzliche Regelungen „Vertraulichkeit", „Schutz vor unbefugter Kenntnisnahme" etc. fordern. Wie die oben aufgezählten Beispiele zeigen, ist dies vor allem bei sensiblen Daten im Sinne des § 3 IX BDSG der Fall sowie bei sonstigen Daten, die als besonders schutzwürdig angesehen werden, etwa Steuerdaten und Registerdaten.[303]

Dieser Grundsatz ist über den Fall der Übermittlung in allgemein zugänglichen Netzen hinaus auszudehnen auf alle Datenübermittlungen in vergleichbar unsicheren Umgebungen, etwa in WLANs (`Wireless Local Area Network´), die ein Abhören im Vergleich zu drahtgebundenen Netzen deutlich vereinfachen.[304] Dieses Verständnis liegt etwa auch § 6 III S. 1 LDSG Schleswig-Holstein zu Grunde, der Verschlüs-

Meldeverordnung); § 8 I S. 2 Verordnung zur Durchführung des § 61a des Gesetzes über die Alterssicherung der Landwirte (Alterssicherung der Landwirte/Datenabgleichsverordnung); § 1 III Verordnung über die elektronische Übermittlung von für das Besteuerungsverfahren erforderlichen Daten (Steuerdaten-Übermittlungsverordnung); § 2 II S. 2 Verordnung über das Zentrale Vorsorgeregister; § 2 VI S. 2 Verordnung zur Durchführung des Fahrpersonalgesetzes (Fahrpersonalverordnung); §§ 3 II, 9 II und 11 II Verordnung zur Konkretisierung von Anzeige-, Mitteilungs- und Veröffentlichungspflichten sowie der Pflicht zur Führung von Insiderverzeichnissen nach dem Wertpapierhandelsgesetz (Wertpapierhandelsanzeige- und Insiderverzeichnisverordnung); §§ 12 I S. 3 und 18 II S. 3 des Entwurfs eines Gesetzes über Personalausweise und den elektronischen Identitätsnachweis vom 07.10.2008, BT-Drs. 16/10489. Explizit Verschlüsselung fordern dagegen § 34a II S. 3 Hessisches Meldegesetz und § 5 II S. 2 Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (Meldedaten-Übermittlungsverordnung).

303 Ein weiterer Beleg dafür ist das bis 31.12.1999 geltende Krebsregistergesetz (BGBl. I 1994, 3351; jetzt ersetzt durch Landeskrebsregistergesetze), das in den §§ 6 und 7 die Verpflichtung, Identitätsdaten nur asymmetrisch verschlüsselt zu speichern, normierte.

304 Da ein physischer Zugriff hierfür nicht erforderlich ist; nur eine elektromagnetische Abschirmung kann ein externes Abfangen von Funksignalen verhindern; vgl. *Eckert*, IT-Sicherheit, S. 823.

selung bei Datenverarbeitung außerhalb der Räumlichkeiten der datenverarbeitenden Stelle, und damit in weniger sicherer Umgebung, fordert.[305]

b. „Schutz gegen unbefugte Kenntnisnahme" in sog. `sicheren´ Umgebungen

Private, lokale Netze stellen im Gegensatz zu allgemein zugänglichen Netzen nicht per se unsichere Umgebungen dar – wenn sie gegenüber anderen Netzen hinreichend abgeschottet und geschützt sind. Ob neben einem Firewall-System[306] und eventuell weiteren Sicherheitsmaßnahmen auch eine Verschlüsselung von Daten erforderlich ist, dürfte im Einzelfall vom konkreten Sicherheitskonzept einerseits und der Sensibilität der Daten andererseits abhängen. So verlangt etwa § 2 II S. 2 Erste Bundesmeldedatenübermittlungsverordnung *stets* die Verschlüsselung der zu übermittelnden Daten – auch bei unmittelbarer Übertragung zwischen den Meldebehörden.[307] Auch § 10 S. 2 Sozialhilfedatenabgleichsverordnung normiert für jede Datenübermittlung eine Verschlüsselungspflicht.[308] § 2 II S. 1 Steueridentifikationsnummernverordnung nennt als Übermittlungsmedium neben dem Internet ausdrücklich „verwaltungseigene Kommunikationsnetze" und legt in Satz 3 eine Verschlüsselungspflicht fest.[309] *Daraus folgt, dass im Fall der Betroffenheit besonders sensibler Daten oder von Daten mit einem besonders hohen Verknüpfungspotential* (Steueridentifikationsnummer!), *auch bei Übermittlung in lokalen, „sicheren" Netzen eine Verschlüsselungspflicht vorliegt*. Für diese Sichtweise spricht auch § 17 Ia S. 2 und 3 Hessische Beihilfenverordnung:

> „Wird für den Festsetzungsbescheid die elektronische Form gewählt, so sind dessen Daten mit einem geeigneten Verfahren *zu verschlüsseln*. Dies gilt auch für sonstige Mitteilungen der Festsetzungsstelle, *soweit die Art der personenbezogenen Daten dies erfordert*. [Hervorhbg. d. d. Verf.]"

305 § 6 III S. 1 Landesdatenschutzgesetz Schleswig-Holstein: „Werden personenbezogene Daten mit Hilfe informationstechnischer Geräte von der datenverarbeitenden Stelle außerhalb ihrer Räumlichkeiten verarbeitet, sind die Datenbestände zu verschlüsseln."

306 Siehe dazu ausführlich *Eckert*, IT-Sicherheit, S. 646 ff.

307 § 2 II Erste Bundesmeldedatenübermittlungsverordnung: „Datenübertragungen erfolgen zwischen den Meldebehörden unmittelbar oder über Vermittlungsstellen. Die zu übermittelnden Daten sind mit einer fortgeschrittenen elektronischen Signatur nach § 2 Nr. 2 des Signaturgesetzes zu versehen und zu verschlüsseln."

308 § 10 S. 2 Sozialhilfedatenabgleichsverordnung: „Die Daten sind vor dem Versand mit dem von der Vermittlungsstelle zur Verfügung gestellten Verschlüsselungsprogramm zu verschlüsseln und zu signieren."

309 § 2 II Steueridentifikationsnummernverordnung: „Die Datenübermittlungen des Bundeszentralamts für Steuern an die Meldebehörden nach § 139b Abs. 6 Satz 5 und Abs. 7 Satz 2 der Abgabenordnung erfolgen durch Datenübertragung über verwaltungseigene Kommunikationsnetze oder über das Internet. […] Die zu übermittelnden Daten sind mit einer fortgeschrittenen elektronischen Signatur nach § 2 Nr. 2 des Signaturgesetzes zu versehen und nach dem Stand der Technik zu verschlüsseln. […]" Eine parallele Regelung enthält auch § 6 IIa S. 1 und 3 Zweite Bundesmeldedatenübermittlungsverordnung.

3. Verschlüsselung zum Schutz der „Unversehrtheit“ bei Datenübermittlungen (teleologische Auslegung)

Über die Vertraulichkeit hinaus ist bei Datenübermittlungen auch die „Unversehrtheit“ der Daten zu gewährleisten; vgl. etwa § 24c VI S. 1 KWG:[310]

> „Das Kreditinstitut und die Bundesanstalt haben dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der abgerufenen und weiter übermittelten Daten gewährleisten.“

Zum Teil wird auch vom Schutz „gegen den unbefugten Zugriff Dritter“ gesprochen; etwa in § 21a S. 1 BZRG:

> „Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit diese Form der Datenübermittlung unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen wegen der Vielzahl der Übermittlungen oder wegen ihrer besonderen Eilbedürftigkeit angemessen ist und wenn gewährleistet ist, dass die Daten gegen den unbefugten Zugriff Dritter bei der Übermittlung wirksam geschützt werden.“

„Schutz der Unversehrtheit“ wie „Schutz gegen unbefugte Zugriffe Dritter“ bedeutet dabei in teleologischer Auslegung nichts anderes als Schutz der Integrität.[311]

Bei Datenübermittlungen geht es regelmäßig um Integritätsschutz in unsicheren Umgebungen. Zum Schutz vor unbemerkter Veränderung der übermittelten Daten sind kryptographische Hashfunktionen und `*Message Authentication Codes*´, die neben Hashverfahren auch einen geheimen kryptographischen Schlüssel verwenden, zwingend erforderlich. Integritätsschutz in unsicheren Umgebungen kann nur mit Hilfe von Verschlüsselungsverfahren gewährleistet werden. *Die Adressaten von Normen, die die Gewährleistung der Unversehrtheit der Daten bei Datenübermittlungen verlangen, müssen nach derzeitigem Stand der Technik Verschlüsselungsverfahren einsetzen.*

310 Ebenso auch § 89a VIII AufenthG; § 78a II S. 2 BNotO; § 16a VI S. 1 GenTG; § 17 II S. 2 SchwarzArbG; § 493 I S. 2 StPO; § 30a II Nr. 1 StVG; § 36 V Nr. 2 StVG; § 53 II Nr. 1 StVG; § 6 Verordnung über das datenbankgestützte Informationssystem über Medizinprodukte des Deutschen Instituts für Medizinische Dokumentation und Information; § 4 I S. 1 Altersvorsorge-Durchführungsverordnung; § 28 VI S. 3 Verordnung über den Schutz vor Schäden durch Röntgenstrahlen; § 6 I S. 2 Auslandsadoptions-Meldeverordnung; § 8 I S. 2 Alterssicherung der Landwirte/Datenabgleichsverordnung; § 2 VI S. 2 Fahrpersonalverordnung; § 3 II und § 9 II Wertpapierhandelsanzeige- und Insiderverzeichnisverordnung; § 12 I S. 3 des Entwurfs eines Gesetzes über Personalausweise und den elektronischen Identitätsnachweis vom 07.10.2008, BT-Drs. 16/10489.

311 Wobei der „Schutz gegen unbefugte Zugriffe Dritter“ auch eine Vertraulichkeitskomponente aufweist, da das automatisierte Abrufverfahren laut Gesetzesbegründung (BR-Drs. 15/01, S. 20) dem nach § 488 StPO nachgebildet werden sollte.

4. Verschlüsselung zum Schutz der „Authentifizierung“ (teleologische Auslegung)

Teilweise wird auch die „Authentifizierung der übermittelnden und empfangenden Stelle“[312] oder die „Authentizität der übermittelnden und empfangenden Stelle“[313] gefordert. Maßnahmen der Authentifikation erfordern häufig, aber nicht immer den Einsatz von Verschlüsselungsverfahren.[314] Soweit biometrische Verfahren zur Authentifikation eingesetzt werden, ist der Einsatz von Verschlüsselung nicht zwingend, im Übrigen allerdings schon. *Der Kontext mit Datenübermittlungen in den genannten Normen spricht aber stark für ein Sicherheitskonzept, das den Einsatz von Verschlüsselung voraussetzt*.[315]

5. Verschlüsselung zum Schutz der „Zurechenbarkeit“ (teleologische Auslegung)

§ 78a II S. 2 BNotO, § 4 III S. 11 FPersG und § 2 VI S. 2 Fahrpersonalverordnung fordern neben der Vertraulichkeit und der Unversehrtheit übermittelter Daten auch deren „Zurechenbarkeit“. Zurechenbarkeit setzt zum einen eine sichere Authentifikation von Subjekten voraus.[316] Daraus wird sich häufig die Notwendigkeit von Verschlüsselungsverfahren ergeben. Zurechenbarkeit beinhaltet aber auch die Komponente der „Nicht-Abstreitbarkeit“ oder „Verbindlichkeit“ (*`non repudiation´*),[317] die wiederum über digitale Signaturverfahren und damit ebenfalls durch Verschlüsselung sichergestellt wird. *Soweit wie hier die Zurechenbarkeit bei Datenübertragungen gewährleistet werden soll, erwächst – nach dem derzeitigen Stand der Technik – aus der Zurechenbarkeitsanforderung eine Pflicht zum Einsatz von Verschlüsselung.*

6. Verschlüsselung zum Schutz „gegen unbefugte Nutzung“?

Die Rechtsgrundlage für die Online-Durchsuchung in § 20k BKAG[318] verlangt in ihrem Abs. 2, S. 2 besondere Schutzmaßnahmen hinsichtlich der Infiltrationssoftware, um diese technisch gegen unbefugte Nutzung zu sichern:

312 § 4 I S. 1 Altersvorsorge-Durchführungsverordnung.
313 § 6 I S. 2 Auslandsadoptions-Meldeverordnung; § 8 I S. 2 Alterssicherung der Landwirte/Datenabgleichsverordnung.
314 Siehe oben unter B.II.3.a.
315 Die geforderte Authentifizierung von empfangender und übermittelnder Stelle legt die Vermutung nahe, dass es um eine wechselseitige Authentifikation in verteilten Systemen geht. Techniken zur Authentifikation in verteilten Systemen basieren sämtlich auf Verschlüsselungsverfahren; vgl. die einzelnen Verfahren bei *Eckert*, IT-Sicherheit, S. 488 ff.
316 *Dierstein,* InfSpekt 2004, 343, 349.
317 *Dierstein,* InfSpekt 2004, 343, 349; *Eckert*, IT-Sicherheit, S. 11.
318 Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz - BKAG) vom 07.07.1997

„Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen."[319]

Da die Norm ein staatliches Eindringen in informationstechnische Systeme des Einzelnen mittels spezieller Programme gestattet, müssen diese Programme technisch gegen Missbrauch durch Dritte geschützt werden. Zu prüfen ist, ob der technische Schutz vor Missbrauch im Rahmen der Online-Durchsuchung den Einsatz von Verschlüsselungsverfahren erforderlich macht. Dritte könnten vor allem versuchen, die ausgespähten Daten an einen anderen Server, auf den sie selbst Zugriff haben, übermitteln zu lassen[320] oder die Online-Durchsuchungssoftware in anderer Weise zu manipulieren. Voraussetzung wäre aber jedenfalls die Entdeckung der Durchsuchungssoftware sowie deren Analyse (im Hinblick darauf, wie sie manipuliert werden kann). Zumindest die Analyse soll nach Angaben des Innenministeriums durch Verschlüsselungsverfahren „nahezu unmöglich gemacht" werden.[321] Darüber, wie der technische Missbrauchsschutz im Übrigen ausgestaltet werden soll, existieren keine Angaben, so dass dies einer näheren Beurteilung auch nicht zugänglich ist. Entscheidend dürfte der Hinweis sein, dass eine Manipulation der Durchsuchungssoftware extrem aufwändig wäre – zumal Schadprogramme mit entsprechenden Funktionen via Internet frei verfügbar sind und zum Teil direkt genutzt werden können.[322] Inwieweit für den technischen Missbrauchsschutz zwingend Verschlüsselungsverfahren genutzt werden müssen, kann hier im Ergebnis nicht beurteilt werden.

(BGBl. I S. 1650), zuletzt geändert durch Artikel 1 des Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25.12.2008 (BGBl. I 3083).

319 So auch der am 08.12.2009 verabschiedete neue § 15b II S. 2 HSOG (Art. 1, Ziffer 8 des Gesetzesentwurfs vom 30.06.2009, Drs. 18/861); ähnlich auch bereits die Vorschriften zur Telekommunikationsüberwachung in § 14 I, II TKÜV: „(1) Der Verpflichtete hat die von ihm zu treffenden Vorkehrungen zur technischen und organisatorischen Umsetzung von Anordnungen, insbesondere die technischen Einrichtungen zur Steuerung der Überwachungsfunktionen und des Übergabepunktes nach § 8 einschließlich der zwischen diesen befindlichen Übertragungsstrecken, nach dem Stand der Technik gegen unbefugte Inanspruchnahme zu schützen. (2) Die Überwachungskopie ist durch angemessene Verfahren gegen eine Kenntnisnahme durch unbefugte Dritte zu schützen. […]"

320 Die Datensicherheit bei der Übermittlung regelt § 20k II S. 3 BKAG: „Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen."

321 Bundesministerium des Innern, Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien und AG Neue Medien, verfügbar unter: http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (06.01.2009), S. 6 und16.

322 Bundesministerium des Innern, Fragenkatalog des Bundesministeriums der Justiz, verfügbar unter: http://netz politik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (31.10.2007), S. 21 sowie Fox, Stellungnahme zur "Online-Durchsuchung", verfügbar unter: http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf (30.12.2008), S. 15.

7. Verschlüsselung als „technische und organisatorische Maßnahme“ im Datenschutzrecht (grammatische und teleologische Auslegung)

Verschlüsselungsverfahren können über die Fälle von Datenübermittlungen hinaus auch im Übrigen als „technische und organisatorische Maßnahmen“ im Sinne der Anlage zu § 9 S. 1 BDSG erforderlich sein:

> „Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,
>
> 1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
>
> 2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
>
> 3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
>
> 4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
>
> 5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
>
> 6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
>
> 7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
>
> 8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
>
> Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.“

In den Landesdatenschutzgesetzen existieren entsprechende Normen, in Hessen § 10 II HDSG:

> „Werden personenbezogene Daten automatisiert verarbeitet, ist das Verfahren auszuwählen oder zu entwickeln, welches geeignet ist, so wenig personenbezogene Daten zu verarbeiten, wie zur Erreichung des angestrebten Zwecks erforderlich ist. Außerdem sind Maßnahmen schriftlich anzuordnen, die nach dem jeweiligen Stand der Technik und der Art des eingesetzten Verfahrens erforderlich sind, um zu gewährleisten, daß
>
> 1. Unbefugte keinen Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, erhalten (Zutrittskontrolle),

2. Unbefugte an der Benutzung von Datenverarbeitungsanlagen und -verfahren gehindert werden (Benutzerkontrolle),

3. die zur Benutzung eines Datenverarbeitungsverfahrens Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),

4. personenbezogene Daten nicht unbefugt oder nicht zufällig gespeichert, zur Kenntnis genommen, verändert, kopiert, übermittelt, gelöscht, entfernt, vernichtet oder sonst verarbeitet werden (Datenverarbeitungskontrolle),

5. es möglich ist, festzustellen, wer welche personenbezogenen Daten zu welcher Zeit verarbeitet hat und wohin sie übermittelt werden sollen oder übermittelt worden sind (Verantwortlichkeitskontrolle),

6. personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. durch eine Dokumentation aller wesentlichen Verarbeitungsschritte die Überprüfbarkeit der Datenverarbeitungsanlage und des -verfahrens möglich ist (Dokumentationskontrolle),

8. die innerbehördliche oder innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle)."

Die Datenschutzgesetze enthalten jeweils umfangreiche Kataloge an technischen und organisatorischen Maßnahmen, die zum Schutz personenbezogener Daten zu treffen sind. Für Grundbuchdaten sowie Sozialdaten existieren mit der Anlage zu § 126 I S. 2 Nr. 3 GBO[323] und der Anlage zu § 78a SGB X[324] spezielle Kataloge der

323 Anlage zu § 126 Abs. 1 Satz 2 Nr. 3: „Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind, 1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle), 2. zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle), 3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle), 4. zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle), 5. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle), 6. zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle), 7. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle), 8. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle), 9. zu verhindern, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle), 10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle)."

324 Anlage zu § 78a SGB X: „Werden Sozialdaten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Sozialdaten oder Kategorien von Sozialdaten ge-

erforderlichen technischen und organisatorischen Maßnahmen. Darüber hinaus enthält eine Reihe weitere Gesetze einzelne Normen, die den Schutz personenbezogener Daten regeln (spezielles Datenschutzrecht). Hieraus ergeben sich zum Teil besondere technische und organisatorische Anforderungen.

Die technischen und organisatorischen Maßnahmen werden häufig auch als Datensicherungs- oder Datensicherheitsmaßnahmen bezeichnet.[325] Diese Terminologie nimmt Bezug darauf, dass die einzelnen technischen und organisatorischen Katalogmaßnahmen der Datenschutzgesetze (Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags-, Verfügbarkeits-, Benutzer-, Datenverarbeitungs-, Verantwortlichkeits-, Dokumentations-, Organisationskontrolle, etc.) der Gewährleistung der Schutzziele der IT-Sicherheit dienen.[326] Im Datenschutzrecht steht dabei aber nicht – wie beim IT-Sicherheitsbegriff – das gesamte informationstechnische System im Fokus, sondern es geht – angesichts des datenschutzrechtlichen Anwendungsbereichs auf personenbezogene Daten – nur um die Gewährleistung der Sicherheit von Daten (folglich häufig als Datensicherheit bezeichnet).

Inhaltlich geht es aber jeweils um die Gewährleistung von Vertraulichkeit, Integrität und – in eingeschränktem Maße - Verfügbarkeit:

a. Vertraulichkeit

Aspekte des Vertraulichkeitsschutzes finden sich etwa bei der Zutrittskontrolle nach Nr. 1, der Zugangskontrolle nach Nr. 2, der Zugriffskontrolle nach Nr. 3 und der Weitergabekontrolle nach Nr. 4 der Anlage zu § 9 S. 1 BDSG. Im HDSG beinhalten die Zutrittskontrolle (§10 II S. 2 Nr. 1 HDSG), die Benutzerkontrolle (§10 II S. 2 Nr.

> eignet sind, 1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen Sozialdaten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle), 2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle), 3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Sozialdaten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle), 4. zu gewährleisten, dass Sozialdaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung von Sozialdaten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle), 5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Sozialdaten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle), 6. zu gewährleisten, dass Sozialdaten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können (Auftragskontrolle), 7. zu gewährleisten, dass Sozialdaten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle), 8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Sozialdaten getrennt verarbeitet werden können."

325 So etwa bei *Gola/Schomerus,* BDSG, § 9, Rn. 1.

326 So auch *Gola/Schomerus,* BDSG, § 9, Rn. 2.

2 HDSG), die Zugriffskontrolle (§10 II S. 2 Nr. 3 HDSG)[327] und die Datenverarbeitungskontrolle (§10 II S. 2 Nr. 4 HDSG) Aspekte des Vertraulichkeitsschutzes.

aa) Vertraulichkeit von Kommunikationsinhalten

Für die Gewährleistung der Vertraulichkeit von Kommunikationsinhalten bei Datenübermittlungen sind Nr. 4 der Anlage zu § 9 S. 1 BDSG und – in Hessen – § 10 II S. 2, Nr. 4 HDSG maßgeblich.[328] Auch hier ergibt sich bei ermessensfehlerfreier Anwendung der Normen für Datenübermittlungen in allgemein zugänglichen Netzen eine Verschlüsselungs*pflicht*. Dies zeigt für das BDSG Satz 3 der Anlage zu § 9 S. 1 BDSG:

> „Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren."

Allerdings sind nach § 9 S. 2 BDSG und § 10 I S. 2 HDSG stets nur solche technischen und organisatorischen Maßnahmen erforderlich, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Zugangs-, Zugriffs- und Benutzerkontrolle können auch jenseits von Datenübermittlungen die Verschlüsselung von Daten erfordern.[329] Ob sich die Pflicht zur Zugangs-, Zugriffs- und Benutzerkontrolle in einer Verschlüsselungspflicht konkretisiert, kann nur im Einzelfall entschieden werden, da diese Frage nicht losgelöst vom Gesamt-IT-Sicherheitskonzept beantwortet werden kann. Bei *Betroffenheit besonders sensibler Daten* ergibt sich aber auch hier eine *Verschlüsselungspflicht*.[330]

Dies entspricht auch der jüngsten Rechtsprechung des BVerfG in seiner Entscheidung zur Vorratsdatenspeicherung: Das BVerfG fordert für (im Hinblick auf

327 Ein Beispiel für eine spezialgesetzliche Gewährleistung der Zugriffskontrolle durch Verschlüsselung ist § 99 III S. 1 SGB IV.

328 Sowie die Transportkontrolle im Sinne von Ziffer 9 der Anlage zu § 126 I S. 2 Nr. 3 GBO und die Weitergabekontrolle nach Ziffer 4 der Anlage zu § 78a SGB X.

329 Siehe zu im Einzelnen denkbaren Maßnahmen *Ernestus*, in: *Simitis,* BDSG, § 9, Rn. 68 ff., insbes. 97 f., 108 f. und Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe zum Einsatz kryptografischer Verfahren, verfügbar unter: http://www.lda.brandenburg.de/media/2473/kryptoverfahren.pdf (21.04.2008) 16 f. Dementsprechend wird durch die jüngst beschlossene Datenschutznovelle (vgl. BT-Drs. 16/13657) der Anlage zu § 9, S. 1 folgender Satz 3 hinzugefügt: „Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren."

330 S. dazu oben unter C. II. 2. sowie Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe zum Einsatz kryptografischer Verfahren, verfügbar unter: http://www.lda.brandenburg.de/media/2473/kryptoverfahren.pdf (21.04.2008), S. 16: „Vor allem dann, wenn aufgrund der Sensibilität der Daten oder der besonderen Einsatzbedingungen der IT-Systeme mit anderen Maßnahmen den Risiken bei der Gewährleistung der Vertraulichkeit und Integrität nicht hinreichend entgegen gewirkt werden kann, kommt auch die kryptografische Verschlüsselung des Speicherinhalts oder einzelner Dateien als Maßnahme in Frage."

den Umfang der Datenspeicherung oder die potentielle Aussagekraft der Datenbestände) besonders schutzwürdige Daten „besonders hohe Standards der Datensicherheit“[331] – und leitet daraus eine Verschlüsselungspflicht ab:

> „Die Verfassung gibt nicht detailgenau vor, welche Sicherheitsmaßgaben im Einzelnen geboten sind. Im Ergebnis muss jedoch ein Standard gewährleistet werden, der unter spezifischer Berücksichtigung der Besonderheiten der durch eine vorsorgliche Telekommunikationsverkehrsdatenspeicherung geschaffenen Datenbestände ein besonders hohes Maß an Sicherheit gewährleistet. Dabei ist sicherzustellen, dass sich dieser Standard – etwa unter Rückgriff auf einfachgesetzliche Rechtsfiguren wie den Stand der Technik – an dem Entwicklungsstand der Fachdiskussion orientiert und neue Erkenntnisse und Einsichten fortlaufend aufnimmt. Entsprechend ist vorzusehen, dass die speicherpflichtigen Unternehmen – zum Beispiel auf der Grundlage von in regelmäßigen Abständen zu erneuernden Sicherheitskonzepten – ihre Maßnahmen hieran nachprüfbar anpassen müssen. Das Gefährdungspotential, das sich aus den in Frage stehenden Datenbeständen ergibt, erlaubt es nicht, die beschriebenen Sicherheitsanforderungen einer freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten zu unterwerfen. Wenn der Gesetzgeber eine flächendeckende Speicherung der Telekommunikationsverkehrsdaten ausnahmslos vorschreibt, gehört es zu den erforderlichen Voraussetzungen, dass die betroffenen Anbieter nicht nur ihre Pflicht zur Speicherung, sondern auch die korrespondierenden Anforderungen zur Datensicherheit erfüllen können. Anknüpfend an die sachverständigen Stellungnahmen liegt es nahe, dass nach dem gegenwärtigen Stand der Diskussion grundsätzlich eine getrennte Speicherung der Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffsregime unter Nutzung etwa des Vier-Augen-Prinzips sowie eine revisionssichere Protokollierung sichergestellt sein müssen, um die Sicherheit der Daten verfassungsrechtlich hinreichend zu gewährleisten.“[332]

bb) Vertraulichkeit von Kommunikationsumständen (Anonymität)

Die Kataloge der technisch-organisatorischen Datenschutzmaßnahmen enthalten dagegen keine Vorgaben zur Vertraulichkeit von Kommunikations*umständen* (*Anonymität*). § 9 S. 1 BDSG verweist aber nicht nur „insbesondere“ auf den Katalog der Anlage zu § 9 BDSG, sondern auf alle Vorschriften des Gesetzes. § 3a BDSG normiert die Grundsätze der Datenvermeidung und Datensparsamkeit:[333]

> „§ 3a BDSG [Datenvermeidung und Datensparsamkeit] Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies

331 BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 221.

332 BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 224.

333 Eine parallele Vorschrift gibt es im HDSG nicht. Allerdings ist der Grundsatz der Datenvermeidung und der Datensparsamkeit als übergreifender datenschutzrechtlicher Grundsatz anzusehen, der über das Erforderlichkeitsprinzip (§ 13 I BDSG; § 11 I HDSG) Eingang in die Datenschutzgesetze findet; *Roßnagel*, in: *Roßnagel,* Handbuch Datenschutzrecht, Kap. 1, Rn. 40. Im HDSG findet sich dieser Grundsatz explizit nochmals in § 10 II S. 1 wieder: „Werden personenbezogene Daten automatisiert verarbeitet, ist das Verfahren auszuwählen oder zu entwickeln, welches geeignet ist, so wenig personenbezogene Daten zu verarbeiten, wie zur Erreichung des angestrebten Zwecks erforderlich ist. […]“

möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

Auch wenn Anonymität demnach über § 9 S. 1 BDSG i.V.m. § 3a BDSG als technisch-organisatorische Maßnahme grundsätzlich zu gewährleisten ist, spielt diese Forderung im Hinblick auf Verschlüsselungspflichten keine Rolle.[334] Die Gefahren für die Vertraulichkeit von Kommunikationsumständen beruhen nicht auf der individuellen Konfiguration eines informationstechnischen Systems, sondern auf der Funktionsweise des Internets und der E-Mail-Übermittlung als solcher. Der Einzelne kann daran mit seiner Systemgestaltung im Wesentlichen nichts ändern. Möglichkeiten zum Einsatz von Anonymisierungstechniken bestehen vor allem beim betroffenen Nutzer selbst. Verantwortliche Stellen[335] können allenfalls darauf achten, personenbezogene Daten in möglichst geringem Umfang zu speichern und so bald wie möglich wieder zu löschen. Andere Datensicherheitsinteressen können dem aber zuwiderlaufen, etwa Zwecke der Störungserkennung und Missbrauchsbeseitigung. Jedenfalls werden diese denkbaren Maßnahmen der verantwortlichen Stellen keinesfalls durch Verschlüsselung umgesetzt.

b. Integrität

Der Großteil der aufgezählten technisch-organisatorischen Maßnahmen enthält Aspekte der Integritätssicherung (Ziffern 1 bis 5 der Anlage zu § 9 S. 1 BDSG und § 10 II S. 2, Ziffern 1 bis 5, 7 und 8 HDSG). Der Einsatz von Verschlüsselungsverfahren kommt dabei vor allem zu Zwecken der Zugangs- und Zugriffskontrolle (Rechteverwaltung, Authentifikation, etc.)[336] sowie der Weitergabekontrolle (Hashfunktionen, *`Message Authentication Code´* etc.)[337] in Betracht (vgl. erneut Satz 3 der Anlage zu § 9 S. 1 BDSG). Auch hier kann sich abhängig vom IT-Sicherheits-

334 Die Herstellung von Anonymität ist daher weitgehend dem Selbstdatenschutz überlassen, etwa durch die Nutzung von Anonymisierungsdiensten. Diensteanbieter von Telemedien sind aber nach § 13 VI TMG verpflichtet, anonyme und pseudonyme Nutzung zu *ermöglichen*: „Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren." Anders wäre die Frage nach dem Schutz der Anonymität bei Existenz einer Verpflichtung zur Vorratsdatenspeicherung zu beurteilen. Für eine umfassende Speicherung von Telekommunikationsumständen hat das BVerfG gerade entscheiden, dass diese Datenbestände insbesondere durch Verschlüsselung gesichert werden müssen (s.o.).

335 Verantwortliche Stelle ist nach § 3 VII BDSG „jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt."

336 *Ernestus*, in: *Simitis,* BDSG, § 9, Rn. 97 f. und 108 f.; Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe zum Einsatz kryptografischer Verfahren, verfügbar unter: http://www.lda.brandenburg.de/media/2473/kryptoverfahren.pdf (21.04.2008), S. 16 f. sowie oben unter B.II.3.a.

337 Siehe oben unter B.II.3.b.

konzept und der Sensibilität der betroffenen Daten eine Verschlüsselungspflicht ergeben.

c. Verfügbarkeit

Aspekte der Gewährleistung der Verfügbarkeit finden sich unter den technisch-organisatorischen Maßnahmen der Datenschutzgesetze dagegen nur wenige. Ziffer 7 der Anlage zu § 9 S. 1 BDSG enthält zwar eine Verfügbarkeitskontrolle, § 10 II HDSG kennt dagegen kein entsprechendes Erfordernis. Dies ist insoweit wenig verwunderlich, als die Verfügbarkeit für den Schutz personenbezogener Daten allenfalls geringe Bedeutung hat. Der „Schutz vor unbefugter Vorenthaltung von Informationen" (so die Definition der Verfügbarkeit, s.o. unter B.III.1.a.aa)) ist regelmäßig für den Schutz personenbezogener Daten bedeutungslos. Beeinträchtigungen des Persönlichkeitsrechts des Einzelnen durch den Umgang mit seinen personenbezogenen Daten (so § 1 I BDSG zum Gesetzeszweck) können nicht dadurch entstehen, dass auf Daten *nicht* zugegriffen werden kann. Jedenfalls wird die Verfügbarkeit von Daten nicht mit Hilfe von Verschlüsselungsverfahren gewährleistet, so dass sich daraus keine Verschlüsselungserfordernisse ergeben können.

III. Einfachgesetzliches Verschlüsselungsverbot

Neben den vielfältigen Verschlüsselungs*geboten* existiert allerdings auch ein ausdrückliches einfachgesetzliches Verschlüsselungs*verbot*, und zwar in § 16 VIII Amateurfunkverordnung[338] für den Amateurfunkverkehr:[339]

> „(8) Amateurfunkverkehr *darf nicht zur Verschleierung des Inhalts verschlüsselt werden*; Steuersignale für Erd- und Weltraumfunkstellen des Amateurfunkdienstes über Satelliten gelten nicht als verschlüsselte Aussendungen. Das Aussenden von irreführenden Signalen, von Dauerträgern und von rundfunkähnlichen Darbietungen sowie der Gebrauch internationaler Not-, Dringlichkeits- und Sicherheitszeichen des See- und Flugfunkdienstes ist nicht zulässig. […]"

Entsprechend gestattet § 89 S. 1 TKG – im Gegensatz zum telekommunikationsrechtlichen Fernmeldegeheimnis, § 88 TKG – ein Abhören der Telekommunikation von Funkamateuren.[340] Definitionsgemäß dient der Amateurfunkdienst nicht der in-

338 Verordnung zum Gesetz über den Amateurfunk – Amateurfunkverordnung vom 15.02.2005 (BGBl. I S. 242).

339 Die Funktechnik ist eine drahtlose Übertragungstechnik von Signalen mittels elektromagnetischer Wellen; Wikipedia, Funktechnik, Version vom 07.11.2008, 18.04 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Funktechnik&oldid=52728595. Diese kann auch digital sein; Wikipedia, Amateurfunkdienst, Version vom 28.05.2009, 13.42 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Amateurfunkdienst&oldi d=60518814.

340 § 89 TKG [Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen]: „Mit einer Funkanlage dürfen nur Nachrichten, die für den Betreiber der Funkanlage, Funkamateu-

dividuellen Kommunikation, sondern experimentellen und technisch-wissenschaftlichen Zwecken sowie zur Völkerverständigung und zur Unterstützung von Hilfsaktionen in Not- und Katastrophenfällen (§ 2 Nr. 2 Amateurfunkgesetz[341]). Amateurfunk ist also grundsätzlich an die Allgemeinheit gerichtet. Der Amateurfunk sollte den Telekommunikationsunternehmen keine Konkurrenz machen. Dem entspricht ein Verbot der Nutzung von Amateurfunkstellen zu gewerblich-wirtschaftlichen Zwecken (§ 5 IV Nr. 1 AmateurfunkG) sowie ein Verbot der geschäftsmäßigen Erbringung von Telekommunikationsdiensten (§ 5 IV Nr. 2 AmateurfunkG, wobei Verstöße bußgeldbewehrt sind, § 9 I Nr. 1, b AmateurfunkG).[342] Das oben genannte Verschlüsselungsverbot stellt insoweit sicher, dass diese Verbote auch effektiv staatlich kontrolliert werden können.

Das Verschlüsselungsverbot trifft daher nur Kommunikation, die per Definition nicht vertraulich sein kann. Auch eine Integritäts- oder Authentizitätserwartung kann es für den Amateurfunkverkehr nicht geben. Daher widerspricht das einfachgesetzliche Verschlüsselungsverbot für Amateurfunkverkehr nicht der These, dass der Schutz von Vertraulichkeit und Integrität zwingend den Einsatz von Verschlüsselungsverfahren erfordern.

IV. Einfachgesetzliche Definition der IT-Sicherheit?

Neben den einfachgesetzlichen Verschlüsselungsge- oder –verboten könnte auch ein juristischer IT-Sicherheitsbegriff Bedeutung für den rechtlichen Umgang mit Verschlüsselung haben.

re im Sinne des Gesetzes über den Amateurfunk vom 23. Juni 1997 (BGBl. I S. 1494), die Allgemeinheit oder einen unbestimmten Personenkreis bestimmt sind, abgehört werden. Der Inhalt anderer als in Satz 1 genannter Nachrichten sowie die Tatsache ihres Empfangs dürfen, auch wenn der Empfang unbeabsichtigt geschieht, auch von Personen, für die eine Pflicht zur Geheimhaltung nicht schon nach § 88 besteht, anderen nicht mitgeteilt werden. […]“

341 Gesetz über den Amateurfunk (Amateurfunkgesetz) vom 23.06.1997 (BGBl. I S. 1494).

342 Diese Festlegung allein auf nicht kommerzielle und nicht private Kommunikation zeigt sich deutlich auch in § 8 der Verordnung zur Durchführung des Gesetzes über den Amateurfunk vom 23.03.1949 (WiGBl. S. 21): „[Inhalt der Sendungen] (1) Der Verkehr ist in offener Sprache abzuwickeln. Der internationale Amateurschlüssel und die international gebräuchlichen Betriebsabkürzungen gelten als offene Sprache. (2) Die gesendeten Texte sind auf technische Mitteilungen über die Versuche selbst sowie auf Bemerkungen persönlicher Art zu beschränken, für die wegen ihrer geringen Wichtigkeit die Übermittlung im öffentlichen Telegraphendienst nicht in Betracht kommen würde. (3) Es ist verboten, daß Amateurfunkstationen für die Übermittlung zwischenstaatlicher Nachrichten, die von dritten Personen ausgehen, benutzt werden. Es ist ferner verboten, unanständige, anstößige oder in anderer Weise anzügliche oder beleidigende Äußerungen im Sendeverkehr zu gebrauchen oder deren Gebrauch zu dulden. Kein Amateur darf unkenntlich gemachte Sendungen über seine Station geben oder die Durchgabe dulden. (4) Die Übertragung von Musik oder Schallaufzeichnungen ist nur kurzzeitig zu Modulationsversuchen gestattet. (5) Die Ausstrahlung des unmodulierten oder ungetasteten Trägers maß auf ein Mindestmaß beschränkt werden.“

1. Einfachgesetzliche Definitionen

Eine viel zitierte[343] rechtliche Definition von IT-Sicherheit bietet etwa § 2 II BSIG, der auf die klassischen Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität verweist.[344] Die IT-Sicherheitsleitlinie für die Hessische Landesverwaltung[345] bezieht unter Punkt 3.2 darüber hinaus die Sicherheitsziele Authentizität und Verbindlichkeit ein.[346] Art. 4c) der Verordnung 460/2004/EG zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit nennt dagegen Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit als Schutzziele.[347] Zum Teil wird auch in den datenschutzrechtlichen Katalogen der technischen und organisatorischen Datenschutz- und Datensicherheitsmaßnahmen auf die Schutzziele der IT-Sicherheit Bezug genommen, wie in § 10 II DSG NRW:[348]

> „(2) Dabei sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass
>
> 1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
>
> 2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
>
> 3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
>
> 4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),
>
> 5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),

343 *Sonntag*, IT-Sicherheit kritischer Infrastrukturen, S. 20; *Holznagel*, Recht der IT-Sicherheit, S. 11; *Heckmann,* MMR 2006, 280, 281; *Hullen,* JurPC 128/2008, Rn. 33.

344 § 2 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) vom 14.08.2009 (BGBl. I S. 2821): „(2) Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen 1. in informationstechnischen Systemen oder Komponenten oder 2. bei der Anwendung von informationstechnischen Systemen oder Komponenten."

345 IT-Sicherheitsleitlinie vom 01.12.2004, StAnz 2004, 3827, verfügbar unter: http://www.datenschutz.hessen.d e/Tb33/K11P01.htm (26.02.2008).

346 „3.2 Für den IT-Einsatz sind die Sicherheitsziele Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit im jeweils erforderlichen Maße zu erreichen."

347 Art. 4 Verordnung (EG) Nr. 460/2004 des europäischen Parlaments und des Rates vom 10.03. 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit, ABl. L 77/1 vom 13.03.2004. „c) „Netz- und Informationssicherheit" die Fähigkeit eines Netzes oder Informationssystems, bei einem bestimmten Vertrauensniveau Störungen und rechtswidrige oder böswillige Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit gespeicherter oder übermittelter Daten und entsprechender Dienste beeinträchtigen, die über dieses Netz oder Informationssystem angeboten werden bzw. zugänglich sind; […]"

348 Gesetz zum Schutz personenbezogener Daten (Datenschutzgesetz Nordrhein-Westfalen – DSG NRW) in der Fassung vom 09.06.2000; GV. NRW 2000, 542.

6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz)."

Im Kern geht es auch bei den Katalogen der Kontrollmaßnahmen in der Anlage zu § 9 BDSG bzw. § 10 II HDSG um die Gewährleistung der IT-Sicherheitsziele.[349] Neben die technischen Sicherheitsanforderungen rücken aber in einer juristischen Perspektive auch andere Sicherheitsanforderungen wie Authentizität, Verbindlichkeit, Datensparsamkeit durch Anonymisierung und Pseudomisierung, Transparenz etc., die oben als gesellschaftliche und nicht IT-sicherheitsbedingte Anforderungen klassifiziert wurden. Das jüngste Gesetzgebungsvorhaben aus dem Bereich der IT-Sicherheit, das Bürgerportalgesetz,[350] kehrt dagegen wieder zur Nennung von Schutzzielen, und zwar Vertraulichkeit, Integrität und Authentizität (§ 5 III Bürgerportalgesetz), zurück.[351]

Insgesamt ist festzustellen, dass sich das informationstechnische Nebeneinander von abstrakten Schutzzielen einerseits und konkreten Gefährdungs- und Maßnahmekatalogen andererseits auf einfachgesetzlicher Ebene fortsetzt. Die Vielfalt der technischen IT-Sicherheitsbegriffe setzt sich somit – wenig überraschend – auf rechtlicher Ebene fort.

2. Abhängigkeit vom informationstechnischen „Stand der Technik"

Die einfachgesetzlichen Normen zeigen, dass die enthaltenen rechtlichen Anforderungen auf den informationstechnischen Erkenntnissen beruhen: So fordert der Großteil der einfachgesetzlichen Normen „dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit"[352]. Die Nennung von Schutzzielen oder Kontrollmaßnahmen erfolgt nur zur Ausfüllung und näheren Konkretisierung des Terminus „Stand der Technik". Der rechtliche IT-Sicherheitsbegriff ist also einerseits abhängig vom informationstechnischen IT-Sicherheitsbegriff und Erkenntnisstand:

„Der rechtliche Maßstab für das Erlaubte oder Gebotene wird hierdurch an die Front der technischen Entwicklung verlagert, da die allgemeine Anerkennung und die praktische Bewährung

349 *Gola/Schomerus,* BDSG, § 9, Rn. 2 sowie oben unter II.7.

350 Entwurf eines Gesetzes zur Regelung von Bürgerportalen und zur Änderung weiterer Vorschriften vom 08.04.2009; BT-Drs 16/12598.

351 Auffallend ist, dass „Authentizität" als eigenständiges Schutzziel genannt wird, eine Forderung nach „Verfügbarkeit" aber fehlt. Dabei wäre diese Forderung durchaus naheliegend, schließlich sollen die Bürgerportale einerseits die elektronischen Zustellung (entsprechend den geplanten Ergänzungen in ZPO und Verwaltungszustellungsgesetz) und andererseits (optional; vgl. § 8 BürgerportalG) die sichere Speicherung von Daten ermöglichen. Beide Funktionen müssten voraussetzen, dass die ständige Zugriffsmöglichkeiten des Nutzers vom Diensteanbieter (in seinem Verantwortungsbereich) zu gewährleisten ist.

352 Siehe etwa § 11 II WpAIV; § 24c VI S. 1 KWG; § 4 III S. 12 FPersG – um nur die bereits im Wortlaut zitierten zu nennen. Ausführlich siehe oben unter II.

allein für den Stand der Technik nicht ausschlaggebend sind. Bei der Formel vom Stand der Technik gestaltet sich die Feststellung und Beurteilung der maßgeblichen Tatsachen für Behörden und Gerichte allerdings schwieriger. Sie müssen in die Meinungsstreitigkeiten der Techniker eintreten, um zu ermitteln, was technisch notwendig, geeignet, angemessen und vermeidbar ist."[353]

3. Unabhängigkeit der rechtlichen Risikobewertung

Andererseits trifft das Recht auch eine eigene, unabhängige Bewertung: So wird das geforderte Sicherheitsniveau rechtlich vorgegeben und nur informationstechnisch ausgefüllt:

> „Die Feststellung, ob das im Einzelfall gesetzlich geforderte Maß an `IT-Sicherheit´ gegeben ist, kann immer nur unter Berücksichtigung der Vorgaben des jeweiligen Gesetzes – z.B. § 9 Bundesdatenschutzgesetz (BDSG), § 87 Telekommunikationsgesetz (TKG) – in Verbindung mit den maßgeblichen untergesetzlichen Konkretisierungen erfolgen."[354]

Die Eigenständigkeit zeigt sich auch am rechtlichen Erforderlichkeitsmaßstab (etwa in § 9 S. 2 BDSG[355]). In einer rechtlichen Perspektive werden Schutzzweck und Aufwand gegeneinander abgewogen. In einer technischen Perspektive werden zwar ähnliche Betrachtungen angestellt; so wird zunächst der Schutzbedarf ermittelt (Analyse von denkbaren Schadensszenarien[356] und anschließende Kategorisierung drohender Schäden[357]) und eine Bedrohungsanalyse durchgeführt.[358] Dann findet eine Risikoanalyse und -bewertung statt.[359] Die technische Perspektive fragt dabei aber nur nach der Wirtschaftlichkeit von Maßnahmen: Sind die Kosten einer Schutzmaßnahme höher als möglicherweise drohende Schäden, werden die verblei-

353 BVerfGE 49, 89, 135 f.

354 *Sonntag*, IT-Sicherheit kritischer Infrastrukturen, S. 23 f.

355 § 9 S. 2 BDSG: „Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

356 Die Verletzung von Gesetzen und Beeinträchtigungen des informationellen Selbstbestimmungsrechts stellen zwei der zu analysierenden Schadensszenarien dar; vgl. Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise, verfügbar unter: http://www.bsi.de/literat/bsi_standard/standard_1002.pdf (19.06.2009), S. 49.

357 Einstufung der Auswirkungen in Schutzbedarfskategorien von „niedrig" über „mittel" und „hoch" bis zu „sehr hoch".

358 Ausführlich zu der gesamten Vorgehensweise *Eckert*, IT-Sicherheit, S. 166 ff. sowie Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-3 – Risikoanalyse auf der Basis von IT-Grundschutz, verfügbar unter: http://www.bsi.de/literat/bsi_standard/standard_1003.pdf (19.06.2009) und Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise, verfügbar unter: http://www.bsi.de/literat/bsi_standard/standard_1002.pdf (19.06.2009), S. 49 ff., wobei es auch in diesem Bereich immer wieder abweichende Terminologien gibt.

359 Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-3 – Risikoanalyse auf der Basis von IT-Grundschutz, verfügbar unter: http://www.bsi.de/literat/bsi_standard/standard_1003.pdf (19.06.2009), S. 14 ff.; *Eckert*, IT-Sicherheit, S. 178 f.

bende Gefährdung und das daraus resultierende Risiko schlicht akzeptiert[360] oder das Risiko wird transferiert – etwa an eine Versicherung.[361] Die Wahrscheinlichkeit eines Schadenseintritts ist entscheidend für den Umgang mit bestimmten Risiken.[362] In einer informationstechnischen Betrachtungsweise geht es bei der Frage des Umgangs mit Risiken allein um Wirtschaftlichkeit[363] und Wahrscheinlichkeit.

In einer rechtlichen Perspektive gibt es dagegen so bedeutende Rechtsgüter, dass jeder finanzielle und organisatorische Aufwand zu ihrem Schutz angemessen ist. Schlichte Risikoverlagerung ist keine Option für den rechtlichen Umgang mit drohenden Schäden, da das Recht die Verhinderung des Eintritts von Schäden anstrebt und sich nicht mit der nachträglichen Deckung der ökonomischen Schäden begnügt. Drohende Schäden sind nicht nach ökonomischen Gesichtspunkten,[364] sondern auf Grund von (grund-)rechtlichen Kriterien zu beurteilen. Juristisch wird zwischen Gefahren, Risiken und Restrisiken unterschieden:[365]

a. Gefahr

Gefahren sind dabei Schadensereignisse, deren Eintritt „hinreichend wahrscheinlich“ ist.[366] Wann die Wahrscheinlichkeit des Schadenseintritts danach als hinreichend anzusehen ist, hängt vom Zusammenspiel zwischen Eintrittswahrscheinlichkeit und drohendem Schaden (Schadensausmaß und Rang der betroffenen Rechtsgü-

360 Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-3 – Risikoanalyse auf der Basis von IT-Grundschutz, verfügbar unter: http://www.bsi.de/literat/bsi_standard/standard_1003.pdf (19.06.2009), S. 17: „Die verbleibende Gefährdung und damit auch das daraus resultierende Risiko wird akzeptiert. Gründe für diese Entscheidung können beispielsweise sein: […] Aufwand und Kosten für wirksame Gegenmaßnahmen überschreiten den zu schützenden Wert.“ So auch *Hartmann*, Sichere Kommunikation im Internet, S. 14.

361 Sog. Risiko-Transfer: Das Risiko, das sich durch die verbleibende Gefährdung ergibt, wird an eine andere Institution übertragen, zum Beispiel durch Abschluss eines Versicherungsvertrags oder durch Outsourcing.“; Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-3 – Risikoanalyse auf der Basis von IT-Grundschutz, verfügbar unter: http://www.bsi.de/literat/bsi_standard/standard_1003.pdf (19.06.2009), S. 17.

362 Nach *Hartmann*, Sichere Kommunikation im Internet, S. 14 definiert sich Risiko in einer informationstechnischen Perspektive wie folgt: „Die Wahrscheinlichkeit, mit der eine Bedrohung in der Praxis auftritt, und die Höhe des möglichen Schadens bestimmen das *Risiko*, dem ein System ausgesetzt ist.“

363 Das liegt natürlich wenig an der Informatik an sich, sondern an ihrem Einsatzfeld, das vor allem von wirtschaftlich arbeitenden Individuen und Unternehmen geprägt ist.

364 So auch VG Freiburg, Urteil vom 14.03.1977, Az.: VS II 27/75; NJW 1977, 1645, 1647 für das Atomrecht: „Zu bedenken ist schließlich, daß *wirtschaftliche Aspekte* grundsätzlich keine Rolle spielen dürfen, wenn es um die Frage geht, welche Schutzvorkehrungen erforderlich sind.“

365 Siehe dazu auch *Wahl/Appel*, Prävention und Vorsorge: Von der Staatsaufgabe zur rechtlichen Ausgestaltung, in: *Wahl,* Prävention und Vorsorge, S. 1, 84 ff.

366 Insgesamt zum Gefahrbegriff und seiner Entwicklung *Di Fabio*, Risikoentscheidungen im Rechtsstaat, S. 67 ff. m.w.N. sowie *Preuß*, Risikovorsorge als Staatsaufgabe, in: *Grimm,* Staatsaufgaben, S. 523, 527 ff.

ter) ab: Je höher der drohende Schaden ist, umso geringer kann die Wahrscheinlichkeit seines Eintretens zu bewerten sein, um noch als „hinreichend wahrscheinlich" zu gelten. Umgekehrt stellen auch geringere Schäden eine relevante „Gefahr" dar, wenn deren Verwirklichung sehr wahrscheinlich ist:

> „Im Bereich des Sicherheitsrechts ist von der Rechtsprechung wiederholt entschieden worden, daß an die Eintrittswahrscheinlichkeit eines Schadensereignisses umso geringere Anforderungen zu stellen sind, je schwerer Art und Ausmaß der Schadensfolgen wiegen. Drohen besonders schwerwiegende Konsequenzen, sind also Leben und Gesundheit der Bürger gefährdet, so muß die erforderliche Vorsorge auch für den Fall einer nur entfernten Möglichkeit bzw. einer noch so wenig naheliegenden Wahrscheinlichkeit des Schadenseintritts getroffen werden. Könnte eine große Zahl von Menschen zu Schaden kommen, dann sind auch äußerst unwahrscheinliche Schadensereignisketten zu berücksichtigen."[367]

Liegt danach eine Gefahr vor, müssen (und dürfen) staatliche Gefahrenabwehrmaßnahmen getroffen werden.[368]

b. Risiko

Im Gegensatz zu Gefahren sind Risiken durch ein Element der kognitiven tatsächlichen Unsicherheit gekennzeichnet: Weder drohende Schäden noch deren Eintrittswahrscheinlichkeit sind sicher bestimmbar, da die betreffende Technologie und ihre möglichen (langfristigen) Auswirkungen (noch) nicht hinreichend erforscht sind. Diese Situation ist prägend für den gesamten Bereich des Umwelt- und Technikrechts.[369] Risiken sind daher solche Schadensereignisse, deren Eintritt möglich, aber nicht „hinreichend wahrscheinlich" erscheint.[370] Die Schwelle zur Gefahr wird also

367 VG Freiburg, Urteil vom 14.03.1977, Az.: VS II 27/75; NJW 1977, 1645, 1646 bezüglich einer atomrechtlichen Genehmigung. Vgl. insgesamt zu der im Atomrecht geführten Diskussion *Di Fabio*, Risikoentscheidungen im Rechtsstaat, S. 69 ff. m.w.N.

368 *Di Fabio*, Risikoentscheidungen im Rechtsstaat, S. 70, 106. Auch das BVerfG fordert in BVerfGE 49, 89, 138 – Kalkar I, „daß der Gesetzgeber grundsätzlich jede Art von anlagespezifischen und betriebsspezifischen Schäden, Gefahren und Risiken in Bedacht genommen wissen will, und daß die Wahrscheinlichkeit des Eintritts eines Schadensereignisses, die bei einer Genehmigung hingenommen werden darf, so gering wie möglich sein muß, und zwar um so geringer, je schwerwiegender die Schadensart und die Schadensfolgen, die auf dem Spiel stehen, sein können."

369 Soweit hier auf Rechtsprechung oder Literatur zum Umgang mit den Risiken der Atomenergie verwiesen wird, soll damit keinesfalls eine Parallelität der technologisch bedingten Gefahren von Atom- und Informationstechnologie impliziert werden. Es geht aber jeweils um den rechtlichen und politischen Umgang mit neuen, unerprobten Technologien. Dies wurde gerade für das Atomrecht breit diskutiert (was angesichts der potentiellen katastrophalen Auswirkungen des Einsatzes von Atomkraft wenig verwunderlich ist). Rechtsprechung und Literaturstimmen aus der Atomenergiedebatte können daher Hinweise und Anregungen für einen rechtlichen Umgang mit den Risiken der Informationstechnologie geben.

370 *Preuß*, Risikovorsorge als Staatsaufgabe, in: *Grimm,* Staatsaufgaben, S. 523, 529; *Di Fabio*, Risikoentscheidungen im Rechtsstaat, S. 74, 105.

gerade nicht überschritten. Risiken erfordern staatliche Maßnahmen der Risikovorsorge.[371]

c. Restrisiko

Da trotz derartiger Risikovorsorge Schadensmöglichkeiten der Verwendung neuer, nicht vollständig erprobter Technologien nicht mit letzter Gewissheit ausgeschlossen werden können, werden *Restrisiken* als hinnehmbar eingestuft:[372]

> „Ungewißheiten jenseits dieser Schwelle praktischer Vernunft haben ihre Ursache in den Grenzen des menschlichen Erkenntnisvermögens; sie sind unentrinnbar und insofern als sozialadäquate Lasten von allen Bürgern zu tragen."[373]

Andernfalls könnten neue und komplexe Technologien niemals eingesetzt werden, was den technischen Fortschritt hemmen oder gänzlich lähmen könnte:

> „Die Zumutbarkeit eines solchen Restrisikos wird für den Bereich der friedlichen Nutzung der Kernenergie ebenso wie für andere - durch technische Gefahrenlagen gekennzeichnete - Bereiche (z.B. Straßen-, Eisenbahn- und Luftverkehr) mit der Begründung gerechtfertigt, daß andernfalls das Leben in einer Industriegesellschaft gelähmt und jede – zwangsläufig zunächst unsichere – Entwicklung der Technik gehemmt werden könnten."[374]

Restrisiken sind also solche Risiken, die nach einer Abwägung[375] von potentiellen (verbleibenden) Schadensmöglichkeiten und der Technologie innewohnenden Chancen für zumut- und damit gesellschaftlich und rechtlich hinnehmbar gehalten werden:

> „Ob eine ganz ungewöhnliche Möglichkeit eines Unglücksfalles noch als zu eliminierendes Risiko anzusehen ist, das Vorsorgemaßnahmen erforderlich macht, oder schon dem zulässigen Restrisiko zuzurechnen ist und nicht mehr als „Gefahr" erscheint, kann deshalb auch davon abhängen, ob fundamentale Interessen der Allgemeinheit an lebenswichtiger Versorgung und technischem Fortschritt die Inkaufnahme einer gewissen Risikolage unumgänglich fordern."[376]

Der Begriff des Restrisikos kann also zusammenfassend definiert werden als

> „jene Schwelle der Eintrittswahrscheinlichkeit eines Schadens, unterhalb derer im Hinblick auf die prinzipielle Knappheit von Ressourcen Schutzvorkehrungen nicht mehr geboten sind, weil die Verwirklichungswahrscheinlichkeit der dort angesiedelten Schadensmöglichkeiten als so

371 *Di Fabio*, Risikoentscheidungen im Rechtsstaat, S. 106.

372 *Di Fabio*, Risikoentscheidungen im Rechtsstaat, S. 105. Vgl. zu den verschiedenen Definitionen *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 238.

373 BVerfGE 49, 89, 143.

374 VG Freiburg, Urteil vom 14.03.1977, Az.: VS II 27/75; NJW 1977, 1645, 1647.

375 *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 238 ff. hat überzeugend herausgearbeitet, dass sich letztlich auch hinter dem Restrisikobegriff nichts anderes als die Frage nach der Sozialadäquanz verbirgt und es damit im Kern um eine Abwägungsentscheidung geht: „In Wahrheit geht es nicht um die Negation einer Gefahr, sondern um wertende Betrachtungen, die den Bereich von Gefahren bestimmen sollen, der als zumutbar hinzunehmen sei."; ebenda S. 239; ausführlich dazu auch *Brüning/Helios,* Jura 2001, 155, 158.

376 VG Freiburg, Urteil vom 14.03.1977, Az.: VS II 27/75; NJW 1977, 1645, 1647.

gering angesehen wird, daß Schäden zwar theoretisch, aber nach dem `Maßstab praktischer Vernunft´ auszuschließen sind.“[377]

Dies verdeutlicht, dass die Grenze zwischen Risiko und Restrisiko rein normativ ist:

„Es handelt sich bei der Fixierung des Restrisikos also nicht um einen Vorgang der wissenschaftlich-analytisch mit Hilfe der Wahrscheinlichkeitsmathematik vorgenommenen Ermittlung eines Produkts aus Eintrittswahrscheinlichkeit und Schadensumfang, sondern um eine normative Entscheidung über die Akzeptabilität von Erkenntnisirrtümern, die als Preis für den wissenschaftlich-technischen Fortschritt und seine Segnungen `von jedermann als sozialadäquat hinzunehmen sind´.“[378]

d. Rechtlicher Umgang mit Gefahren und Risiken

Die Grundsatzentscheidung, ob eine bestimmte Technologie angesichts einer derartigen Unsicherheit über das Bestehen und das Ausmaß von Gefahren überhaupt genutzt werden soll, obliegt dem Gesetzgeber:

„Die normative Grundsatzentscheidung für oder gegen die rechtliche Zulässigkeit der friedlichen Nutzung der Kernenergie im Hoheitsbereich der Bundesrepublik Deutschland ist wegen ihrer weitreichenden Auswirkungen auf die Bürger, insbesondere auf ihren Freiheitsbereich und ihren Gleichheitsbereich, auf die allgemeinen Lebensverhältnisse und wegen der notwendigerweise damit verbundenen Art und Intensität der Regelung eine grundlegende und wesentliche Entscheidung im Sinne des Vorbehalts des Gesetzes. Sie zu treffen ist allein der Gesetzgeber berufen.“[379]

Dabei steht ihm – angesichts fehlender abschließender wissenschaftlicher Erkenntnis – ein weiter Einschätzungs- und Prognosespielraum zu. Verändert sich die Gefahreneinschätzung später (etwa aufgrund neuer wissenschaftlicher Erkenntnisse oder veränderter gesellschaftlicher Bewertung[380]), ist der Gesetzgeber nach der Rechtsprechung des BVerfG verpflichtet, erneut tätig zu werden.

„Dieses bisher hingenommene Risiko kann aber durch neue Erkenntnisse für die Zukunft durch den Gesetzgeber neu bewertet und als nicht mehr hinnehmbar eingestuft werden, wenn dazu fachwissenschaftliche Erkenntnisse über ein erhöhtes Gefährdungsrisiko vorliegen oder auch eine grundlegend andere Bewertung dieser Risiken in weiten Teilen der Bevölkerung festzustellen ist, die vom Gesetzgeber aufgegriffen werden.“[381]

Das Recht trifft somit eine eigene Abwägung der Risiken und Chancen noch nicht (vollständig) erprobter neuer Technologien. Die (Informations-)Technik ist zwar Erkenntnisquelle für mögliche Schäden, die Entscheidung für oder gegen den Einsatz

377 *Preuß*, Risikovorsorge als Staatsaufgabe, in: *Grimm,* Staatsaufgaben, S. 523, 529 f.
378 *Preuß*, Risikovorsorge als Staatsaufgabe, in: *Grimm,* Staatsaufgaben, S. 523, 530.
379 BVerfGE 49, 89, 127 – Kalkar I.
380 So war früher etwa Passivrauchen sozialadäquat und wurde als bloße Belästigung angesehen, heute werden zum Schutz von Leben und Gesundheit umfassende Nichtraucherschutzgesetze erlassen; Beispiel nach *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 107.
381 *Stüer/Loges,* NVwZ 2000, 9, 12.

einer Technologie und dessen Bedingungen trifft das Recht aber eigenständig, unter Zugrundelegung eigenständiger, juristischer Maßstäbe.

4. Zusammenfassung: IT-Sicherheit in einer juristischen Perspektive

Insoweit bietet eine juristische Perspektive zwar *keinen eigenen Begriff* der IT-Sicherheit, denn dieser ist durch das informationstechnische Verständnis von IT-Sicherheit (vor)geprägt. Eine juristische Perspektive bietet aber eine *eigenständige Interpretation von IT-Sicherheit*, soweit es um die Festlegung des erforderlichen Sicherheitsniveaus, die Bestimmung der notwendigen Gefahrenabwehr- und Risikovorsorgemaßnahmen sowie der hinnehmbaren Restrisiken geht. Die zu Grunde liegende Abwägungsentscheidung basiert nur zum Teil auf wirtschaftlichen (so etwa wenn in § 9 S. 2 BDSG der „Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck“ stehen muss), in der Hauptsache aber auf (grund)rechtlichen Kriterien.

Die wesentlichen Ergebnisse dieses Teil 1 und die weitere Prüfungsfolge sollen im folgenden Teil 2 konturiert werden.

Teil 2: Verschlüsselungsdilemma und staatliche Regelungsoptionen – Vorstellung der Szenarien und Strukturierung der weiteren Prüfung

A. Zentrale Erkenntnisse über Verschlüsselung: das Verschlüsselungsdilemma

I. (Einmal-)Verschlüsselung als „absolut sicheres" Verfahren

Verschlüsselung ist ein „absolut sicheres" Verfahren. Die Verwendung des Terminus „absolut sicher" scheint dabei auf den ersten Blick nicht ganz korrekt. Die meisten Verschlüsselungsalgorithmen können (theoretisch) morgen gebrochen werden. Mit der Einmalverschlüsselung (*`One-Time-Pad´*) steht aber jedenfalls *ein mathematisch beweisbar sicheres* Verfahren zur Verfügung. Ein Brechen dieses Verfahrens ist nicht möglich. Im Übrigen basiert die Sicherheit von Verschlüsselungsverfahren auf den Faktoren Zeit und Wahrscheinlichkeit.

Wenn hier von „absoluter Sicherheit" gesprochen wird, ist dies als Hinweis auf die Brisanz zu verstehen, die der Einsatz von Verschlüsselung (sicherheits-)politisch mit sich bringt. Verschlüsselungsverfahren bieten höchst effektive Sicherheit gegenüber jedem denkbaren Angreifer – unabhängig von den diesem zur Verfügung stehenden Ressourcen. *Selbst die staatlichen Sicherheitsbehörden können starke Verschlüsselungsverfahren nicht brechen*. Zwar kann vermutet werden, dass es bereits in der Vergangenheit Techniken und Sicherheitsverfahren gegeben hat, die auch gegenüber dem Staat wirksam waren. Die Besonderheit bei Verschlüsselungsverfahren besteht darin, dass sie – selbst bei Verwendung großer Schlüssellängen und hoch effektiver Algorithmen – eine *Massen*technologie darstellen. Moderne Implementierungen von Verschlüsselungsverfahren können dabei nicht nur auch *von technischen Laien* genutzt werden; derartige Verfahren sind auch via Internet tatsächlich *für jedermann verfügbar*.

Die dadurch drohende massenhafte Verwendung von Verschlüsselungstechnologien stellt traditionell vorhandene staatliche Kenntnisnahmemöglichkeiten nachhaltig in Frage. Diese Konstellation einer massenhaften Infragestellung staatlicher Zugriffsmöglichkeiten ist soweit ersichtlich eine *bisher einzigartige Erscheinung*. Dies rechtfertigt aus Sicht der Verfasserin die Einordnung von Verschlüsselungsverfahren als (nach der hier verwendeten Terminologie) „absolut sichere" Verfahren – im Gegensatz zur bisher allein verfügbaren „relativen" Sicherheit, die zwar gegenüber Dritten, (auf Dauer) aber nicht gegenüber dem Staat Wirksamkeit entfalten konnte.

II. Verschlüsselung zum Schutz der Vertraulichkeit von Kommunikationsinhalten in der digitalen Welt

Dabei sind Verschlüsselungsverfahren im digitalen Zeitalter zum Schutz der Vertraulichkeit von Kommunikationsinhalten unabdingbar:

Einerseits nimmt die Präsenz von Informations- und Kommunikationstechnologie im Alltag stetig weiter zu: Die E-Mail ist fester Bestandteile des privaten wie beruflichen Kommunikationsverhaltens vieler Menschen geworden. Aus der Arbeitswelt sind Computer nicht mehr wegzudenken. Die Mehrzahl der Privathaushalte verfügt heutzutage über mindestens einen PC, der für die verschiedensten Anwendungen genutzt wird und daher vielfältige private Daten enthält.

Andererseits sind die verwendeten Technologien sowie alle informationstechnischen Systeme, soweit sie über einen Internetzugang verfügen, (theoretisch) grundsätzlich angreifbar und auch (praktisch) tatsächlich Gegenstand von Angriffen: E-Mails können aufgrund der dezentralen Netzwerkarchitektur und des zur Erhöhung der Ausfallsicherheit gewählten Übertragungsmodus von einer unbekannten Zahl Dritter gelesen und unbemerkt verändert werden. Informationstechnische Systeme sind via Internet täglich den Angriffen von Hackern ausgesetzt. Selbst informationstechnische Systeme, die mit Virenscanner, Firewall etc. ausgestattet sind und ordnungsgemäß gewartet werden (Software-Updates, Patches etc.), gewähren keinen absoluten Schutz der Vertraulichkeit. Die Ausnutzung soeben bekannt gewordener Sicherheitslücken (`*Zero-Day Exploits´*) oder bisher unbekannter Sicherheitslücken (`*Less-Than-Zero-Day Exploits´*) macht alle informationstechnischen Systeme grundsätzlich angreifbar. Einen absoluten Schutz vor den zuletzt genannten Bedrohungen gibt es dabei nicht.

Der Einsatz von Verschlüsselungstechnologien wird damit zum zentralen Instrument des Vertraulichkeitsschutzes. Nur durch den Versand verschlüsselter E-Mails kann sichergestellt werden, dass die Kommunikation nicht auf dem Versandweg von Dritten abgefangen und mitgelesen wird. Gleichzeitig ist die theoretische Beherrschung und praktische Nutzung etwa von E-Mail-Kommunikation zu einer Frage gesellschaftlicher In- oder Exklusion geworden. Die Nicht-Nutzung der modernen Informations- und Kommunikationstechnologien hat zunehmend reale soziale Folgen für den Einzelnen, so dass nur noch bedingt von einer „freiwilligen“ Entscheidung für oder gegen die Nutzung dieser Technologien gesprochen werden kann. Zum Teil, etwa im beruflichen Umfeld, wird überhaupt keine Freiwilligkeit mehr gegeben sein. Verschlüsselung ist die einzige Möglichkeit, Vertraulichkeit von Kommunikation in der digitalen Welt zu gewährleisten.

III. Verschlüsselung zur Umsetzung weiterer Aspekte von IT-Sicherheit

Verschlüsselungsverfahren dienen neben dem Schutz der Vertraulichkeit von Kommunikation auch der Verwirklichung weiterer Aspekte von IT-Sicherheit:

- Verschlüsselungsverfahren sichern die *Integrität* von Daten. Verschlüsselungsverfahren werden etwa für „die gegenseitige Authentifikation zwischen IT-Systemen, die Absicherung der Zugangskontrolle durch `*challenge-respone´*-Verfahren, die Rechteverwaltung in Zertifikaten, zur Integritäts- und Urheberschaftssicherung von Software-Komponenten“[382] eingesetzt.
- Verschlüsselungsverfahren werden insbesondere auch zur Gewährleistung der *Authentizität* (als Teilaspekt der Integrität) verwendet. Eine mit einer digitalen Signatur unterzeichnete Nachricht gewährleistet zum einen die *Authentizität dieser Nachricht* (Die Nachricht wurde nicht verändert.) und zum anderen die *Authentizität des Absenders* (Absender kann nur derjenige sein, der im Besitz des Schlüssels ist.[383]).[384]
- Verschlüsselungsverfahren können auch *Anonymität* und damit die *Vertraulichkeit von Kommunikationsumständen* gewährleisten: Anonymisierungsdienste wie Tor (`*The Onion Router´*) und JAP (`*Java Anon Proxy´*) ermöglichen anonymes Surfen im Internet. Unabhängig davon, ob die verwendeten Verfahren zur Herstellung von Anonymität auf Mixkaskaden oder auf ein Netzwerk virtueller Tunnel zurückgreifen, ist die Verschlüsselung der Verbindungen jeweils zentraler Bestandteil der Anonymisierungsverfahren.

Verschlüsselung wird daher auch als Kerntechnologie des Cyberspace („core technology of cyberspace“[385]) bezeichnet. Verschlüsselungsverfahren mögen nicht die einzige denkbare Option darstellen, die genannten IT-Sicherheitsziele zu erreichen. Nach derzeitigem Stand der Technik ist es aber *de facto die essentielle Technik* zur Umsetzung von IT-Sicherheit. Dabei mag es sich tatsächlich um die beste Option handeln oder eventuell auch nur um die am besten bekannte Option.

Daraus ergibt sich für die Zukunft folgende *Perspektive*: Es mag in Zukunft durchaus andere technische Optionen geben, die leisten, was heute Verschlüsselungsverfahren leisten. *Soweit diese technischen Optionen ebenfalls über die hier als determinierend beschriebenen Eigenschaften von Verschlüsselungsverfahren verfügen, gelten die rechtlichen Wertungen gleichermaßen.*

IV. Fazit: Ambivalenz von Verschlüsselung

Diese Erkenntnisse führen im Zusammenspiel zu folgender Situation: Der Einzelne ist Teil einer digitalisierten Gesellschaft. Digitale Informationen besitzen einen hohen (wirtschaftlichen, gesellschaftlichen etc.) Stellenwert. Diese Informationen kön-

382 *Hammer*, Die 2. Dimension der IT-Sicherheit, S. 51 jeweils mit weiteren Nachweisen.

383 Damit ist die Authentizität des Absenders nur insoweit garantiert als gewährleistet ist, dass der private Schlüssel einer Person auch tatsächlich nur dieser Person zugänglich ist.

384 Vgl. dazu *Schwenk*, Sicherheit und Kryptographie im Internet, S.6, der neben der digitalen Signatur auch auf `*Message Authentication Codes´* (MAC) als weitere Option hinweist, welche aber ebenfalls auf Verschlüsselungsverfahren basiert.

385 *Schneier*, Secrets and Lies, S.85.

nen effektiv nur durch den Einsatz von Verschlüsselungstechnologien gegen unbefugte Kenntnisnahme geschützt werden. Ohne Verschlüsselung ist die Möglichkeit unbefugter Kenntnisnahme in der digitalen Welt nicht die Ausnahme, sondern allgegenwärtige Regel. Durch den Einsatz von Verschlüsselungsverfahren wird aber nicht nur die illegale und illegitime Kenntnisnahme unbefugter Dritter, sondern auch die – bei Vorliegen der gesetzlichen Voraussetzungen – legale und legitime Kenntnisnahme der staatlichen Sicherheitsbehörden im Wege strafprozessualer[386] oder präventiver Überwachungsmaßnahmen unterbunden.

Es handelt sich um eine sog. `Dual-Use-Technologie´, d.h. eine Technologie mit doppeltem Verwendungszweck. Nach der Dual-Use-Verordnung[387] werden zivile und militärische Zwecke unterschieden (Art. 2 Nr. 1 Dual-Use-Verordnung[388]) und alle Dual-Use-Güter – auch Verschlüsselungsverfahren – einer Exportkontrolle unterworfen.[389] Etwas weiter gefasst können Dual-Use-Technologien auch als Techno-

386 Die Verwendung des Begriffs der strafprozessualen Maßnahmen als Gegenstück zu den präventiven Maßnahmen ist der zunehmenden Bedeutung der Strafverfolgungsvorsorge geschuldet: Die Vorsorge für die Verfolgung von Straftaten erfolgt zeitlich präventiv, ist aber inhaltlich auf das repressive Strafverfahren ausgerichtet. Dadurch wird die begriffliche Trennung „präventiv – repressiv" aufgeweicht. Inhaltlich gehören Maßnahmen zur Strafverfolgungsvorsorge nach der Rechtsprechung des BVerfG (BVerfG, Urteil vom 27.07.2005, Az.: 1 BvR 668/04, Rn. 99 ff.) zum gerichtlichen Verfahren, also in den Anwendungsbereich der StPO. Die Verwendung des Terminus „strafprozessuale Überwachungsmaßnahmen" soll verdeutlichen, dass es neben präventiven und repressiven Maßnahmen auch die Zwischenform der Strafverfolgungsvorsorge gibt, die inhaltlich in der StPO zu verorten wäre. Siehe zur Kritik an der Aufweichung der Grenzziehung zwischen Prävention und Repression durch die Figur der Strafverfolgungsvorsorge *Kutscha*, Innere Sicherheit – Föderale Kompetenzverteilung, Unitarisierung und Internationalisierung, in: *Roggan/Kutscha,* Handbuch zum Recht der Inneren Sicherheit, S. 78, 82 ff.

387 Verordnung (EG) Nr. 428/2009 des Rates vom 5. Mai 2009 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck, ABl. Nr. L 134, S. 1 vom 29.05.2009.

388 Art. 2 Dual-Use-Verordnung 428/2009: „Im Sinne dieser Verordnung bezeichnet der Begriff 1. "Güter mit doppeltem Verwendungszweck" Güter, einschließlich Datenverarbeitungsprogramme und Technologie, die sowohl für zivile als auch für militärische Zwecke verwendet werden können; darin eingeschlossen sind alle Waren, die sowohl für nichtexplosive Zwecke als auch für jedwede Form der Unterstützung bei der Herstellung von Kernwaffen oder sonstigen Kernsprengkörpern verwendet werden können; […]"

389 Auf internationaler Ebene existiert mit dem *`Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies´* ein entsprechendes multilaterales Exportkontroll-Regime. Mitgliedstaaten des Wassenaar-Abkommens sind derzeit (Stand Mai 2010) Argentinien, Australien, Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Italien, Japan, Kanada, Kroatien, Lettland, Litauen, Luxemburg, Malta, Neuseeland, Niederlande, Norwegen, Österreich, Polen, Portugal, Republik Korea, Rumänien, Russland, Schweiz, Schweden, Slowakei, Slowenien, Südafrika, Spanien, Tschechien, Türkei, Ukraine, Ungarn, das Vereinigte Königreich und die Vereinigten Staaten.; vgl. http://www. wassenaar.org. Siehe zum Wassenaar-Abkommen auch *Kuner*, in: *Hoeren/Sieber,* Handbuch Multimedia-Recht, Teil 17, Rn. 17 ff.; *Beucher/Schmoll,* CR 1999, 529, 530 f.

logien verstanden werden, die sowohl erwünschte als auch unerwünschte Verwendungszwecke haben – Dual-Use-Technologien sind per definitionem ambivalent.[390]

Verschlüsselung ist insoweit paradigmatisches Beispiel: Verschlüsselungstechnologien haben den erwünschten Zweck der Gewährleistung von IT-Sicherheit sowie den unerwünschten Zweck, Daten auch für einen erwünschten Zugriff (staatlicher Sicherheitsbehörden) unknackbar zu sichern. Dies wird hier als das Verschlüsselungsdilemma bezeichnet.

B. Optionen des staatlichen Umgangs mit Verschlüsselung

Angesichts dieses Verschlüsselungsdilemmas drängt sich die Frage auf, wie der Staat auf diese Situation reagieren kann bzw. welche Optionen des staatlichen Umgangs mit Verschlüsselung existieren. Die Regelungsoptionen werden hier in fünf paradigmatischen Szenarien verdichtet:

I. Absolutes Verschlüsselungsverbot

Einfachste und zugleich radikalste Option wäre, den Einsatz von Verschlüsselungsverfahren vollständig zu verbieten (Teil 3):

Szenario 1 (absolutes Verschlüsselungsverbot)
Staat S verbietet Verschlüsselungsverfahren.

So existiert etwa in Saudi-Arabien ein vollständiges Verbot von Verschlüsselungsverfahren.[391] Daneben besteht in etlichen Ländern eine Genehmigungspflicht

390 Für den Bereich der Informations- und Kommunikationstechnologien weist *Trute,* JZ 1998, 822, 829 auf weitere Beispiele für die Ambivalenz von Schutzregeln hin, etwa von Filtermaßnahmen (Blockade rechtswidriger Inhalte vs. Zensur) oder von Techniken der Rückverfolgung (Dokumentation und Aufspüren von Persönlichkeitsrechtsverletzungen vs. umfassende Überwachung der Netzkommunikation). Als Beispiel für eine allein an den beabsichtigten Verwendungszweck anknüpfende Unterscheidung von erwünschter (legaler) sowie unerwünschter (illegaler) Verwendung ist an die Strafnorm bezüglich sog. Hacker-Tools zu denken; § 202c: „[Vorbereiten des Ausspähens und Abfangens von Daten] (1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er 1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder 2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. (…)". Das BVerfG hat diese jüngst als verfassungsgemäß angesehen; vgl. BVerfG, Beschluss vom 18.05.2009, Az: 2 BvR 2233/07.

391 So die Hinweise der Princeton Universität zu Import- und Nutzungsrestriktionen für Verschlüsselungssoftware, verfügbar unter: http://www.princeton.edu/itsecurity/services/encryption/travel/ (27.10.2009). Nach den Informationen von Koops, Crypto Law Survey (Stand 01.

für die Verwendung von Verschlüsselungsverfahren, etwa in Belarus (Weißrussland), Kasachstan, Myanmar, der Volksrepublik China, dem Iran, Marokko, der Republik Moldau (Moldawien), Russland und der Ukraine.[392] Eine solche Genehmigungspflicht kann de facto einem Verschlüsselungsverbot gleichkommen – je nachdem, bei welcher Stelle die Genehmigung zu beantragen ist,[393] unter welchen Bedingungen eine Genehmigung erteilt wird und welche Personen realistischerweise einen solchen Antrag stellen können.[394] Es kann davon ausgegangen werden, dass die Genehmigungspraxis tendenziell restriktiv ausfällt – schließlich soll eine verbreitete Nutzung von Verschlüsselung gerade verhindert werden.[395] Für die Masse der Nutzer bedeutet dies de facto ein Verschlüsselungsverbot – da der Staat keinerlei Interesse hat, ihnen eine Genehmigung zu erteilen.[396]

II. Relatives Verschlüsselungsverbot

Etwas weniger restriktiv wäre die Option, die Nutzung bestimmter Verschlüsselungsverfahren, die durch eine Hintertür, ein Schlüsselhinterlegungsmodell oder ein Nachschlüsselmodell die staatliche Kenntnisnahmemöglichkeit im Einzelfall sicher-

07.2008), verfügbar unter: http://rechten.uvt.nl/koops/cryptolaw/cls2.htm (23.10.2009) soll das Verbot aber weitgehend missachtet werden.

392 Vgl. ausführlich dazu Koops, Crypto Law Survey (Stand 01.07.2008), verfügbar unter: http://rechten.uvt.nl/ koops/cryptolaw/cls2.htm (23.10.2009).

393 Zuständig sind meist direkt staatliche Sicherheitsbehörden, vgl. Koops, Crypto Law Survey (Stand 01.07. 2008), verfügbar unter: http://rechten.uvt.nl/koops/cryptolaw/cls2.htm (23.10. 2009).

394 Unter welchen Voraussetzungen Genehmigungen erteilt werden ist unklar. Es kann vermutet werden, dass beispielsweise Unternehmen mit auch in staatlichem Interesse liegendem Geheimhaltungsbedürfnis Genehmigungen erteilt werden würden. Der einzelne Nutzer dürfte dagegen zum Schutz seiner Privatsphäre bereits keinen Antrag bei den Sicherheitsbehörden stellen wollen, jedenfalls wird er vermutlich keine Genehmigung erhalten. Dissidenten steht dieser Weg erst recht nicht offen. Details für einige Staaten bietet *Diehl,* DuD 2008, 243, 246.

395 *Diehl,* DuD 2008, 243, 246 nennt auch Israel als Staat mit Genehmigungspflicht. Israel hat aber kein „klassisches" Genehmigungssystem wie die hier aufgeführten Staaten: Zum einen ist die Genehmigungspraxis laut Koops, Crypto Law Survey (Stand 01.07.2008), verfügbar unter: http://rechten.uvt.nl/koops/cryptolaw/cls2.htm (23.10.2009) sehr liberal, so dass eine Genehmigung (beinahe) immer erteilt wird. Israel ist insofern ein Beispiel dafür, dass ein Genehmigungserfordernis auch als rein administratives Verbot mit Erlaubnisvorbehalt ausgestaltet werden kann. Israel wird hier aber vor allem deswegen nicht in die Liste der Staaten mit Genehmigungspflicht aufgenommen, da die Nutzung von Verschlüsselung ohne eine Genehmigung nicht verfolgt wird und verschiedene generelle Ausnahmetatbestände für die Genehmigungspflicht bestehen: so etwa bei Download von Verschlüsselungssoftware aus dem Internet für den persönlichen Gebrauch.

396 Daher wird die Genehmigungspflicht hier unter die absoluten Verschlüsselungsverbote gefasst: Im Kern sollen möglichst wenige Personen Verschlüsselung nutzen; generell ist Verschlüsselung verboten. Der Ansatz der relativen Verschlüsselungsverbote besteht dagegen darin, die Nutzung von Verschlüsselungsverfahren generell zu gestatten, allerdings nur die Nutzung bestimmter Verfahren.

stellen, zu gestatten und nur den Einsatz anderer Verschlüsselungsverfahren zu untersagen (Teil 4):

Szenario 2 (relatives Verschlüsselungsverbot)
Staat S gestattet nur die Nutzung bestimmter Verschlüsselungsverfahren.

Die Verwendung vor allem von Verschlüsselungsverfahren mit einer verpflichtenden Schlüsselhinterlegung (`*key escrow*´) oder der technisch implementierten Möglichkeit, einen Nachschlüssel zu erzeugen (`*key recovery*´), wurde wesentlich von den Vereinigten Staaten vorangetrieben. 1993 wurde mit dem sog. `*Clipper Chip*´ ein solches System in den Vereinigten Staaten eingeführt – allerdings (zunächst?) auf freiwilliger Basis.[397] Eine Lösung des Verschlüsselungsdilemmas können Verschlüsselungsverfahren mit Schlüsselhinterlegung oder Nachschlüssel aus Sicht der Sicherheitsbehörden aber nur sein, wenn zugleich ein Verbot der Nutzung anderer Verschlüsselungsverfahren besteht – da ansonsten gerade die Inhalte, deren Kenntnisnahme die Sicherheitsbehörden interessiert, vertraulichkeitssicher verschlüsselt sein dürften. Daher wurde auch in den Vereinigten Staaten immer befürchtet, dass die Nutzung von `*key escrow*´- oder `*key recovery*´-Systemen auf längere Sicht *verpflichtend* eingeführt wird. Letztlich konnte sich die `*Clipper*´-Initiative in den Staaten nicht durchsetzen. Aufgrund des internationalen Werbens der Vereinigten Staaten für solche `*key escrow*´/`*key recovery*´-Modelle haben aber andere Staaten diese Ideen aufgegriffen: Frankreich führte 1996 eine Schlüsselhinterlegungspflicht ein, die heute aber nicht mehr in Kraft ist.[398] Auch das Vereinigte Königreich wollte lange Zeit eine Schlüsselhinterlegungspflicht einführen.[399] In Tunesien gilt eine 1997 eingeführte Schlüsselhinterlegungspflicht bis heute, im Zusammenspiel mit einem Genehmigungserfordernis.[400] Auch in Spanien scheint es eine Schlüsselhinterlegungspflicht zu geben.[401]

397 Siehe zu den verschiedenen Entwicklungsstufen der `*Clipper*´-Initiative Koops, Crypto Law Survey (Stand 01.07.2008), verfügbar unter: http://rechten.uvt.nl/koops/cryptolaw/cls2.htm (23.10.2009) sowie Electronic Privacy Information Center, Cryptography and Liberty 2000, verfügbar unter: http://www.stanford.edu/class/msande91si/www-spr04/readings/week6/epic.htm (23.10.2009); ausführlich dazu auch *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 209; *Schneier*, Angewandte Kryptographie, S. 672 ff. sowie allgemein zur Regulierung von Verschlüsselung in den USA *Andrzejak*, Kryptoregulierung, in: *Hoeren/Queck,* Rechtsfragen der Informationsgesellschaft, S. 132, 134 ff.

398 Einzelheiten bei Koops, Crypto Law Survey (Stand 01.07.2008), verfügbar unter: http://rechten.uvt.nl/koops/cryptolaw/cls2.htm (23.10.2009); *Kuner,* in: *Hoeren/Sieber,* Handbuch Multimedia-Recht, Teil 17, Rn. 78; *Kuner*, NJW-CoR 1995, 413, 414.

399 *Kuner,* in: *Hoeren/Sieber,* Handbuch Multimedia-Recht, Teil 17, Rn. 86 ff.

400 Details bei Koops, Crypto Law Survey (Stand 01.07.2008), verfügbar unter: http://rechten.uvt.nl/koops/crypto law/cls2.htm (23.10.2009) sowie Human Rights Watch, False Freedom – Online Censorship in the Middle East and North Africa, 2005, verfügbar unter: http://www.hrw.org/en/reports/2005/11/14/false-freedom (29.10.2009).

401 Koops, Crypto Law Survey (Stand 01.07.2008), verfügbar unter: http://rechten.uvt.nl/koops/cryptolaw/cls2.ht m (23.10.2009) berichtet über Unklarheiten auf Grund einer Gesetzesänderung 2003. Die spanische rechtswissenschaftliche Literatur zeigt aber, dass es sich um ein Schlüsselhinterlegungsmodell handeln dürfte; vgl. *Muñoz Bellvehí/Herreros Margarit/Nolla*

III. Pflicht zur Schlüsselherausgabe

Eine Lösungsoption jenseits von Verschlüsselungsverboten wäre eine Verpflichtung zur Herausgabe der Schlüssel im Einzelfall (Teil 5):

> **Szenario 3 (Herausgabepflicht)**
> Staat S verpflichtet per Gesetz zur Herausgabe von verwendeten Schlüsseln und Passwörtern.

Dies ist ein derzeit in vielen Staaten verfolgter Ansatz zur Lösung des Verschlüsselungsdilemmas. Dabei wird regelmäßig die Entschlüsselung durch den Herausgabepflichtigen, also die Herausgabe der Klartextinformation, der Herausgabe von Schlüsseln oder Passwörtern gleichgestellt. Eine solche Regelung existiert beispielsweise seit 2001 in Australien:[402]

> „3LA Crimes Act 1914 [Person with knowledge of a computer or a computer system to assist access etc.]:
>
> (1) The executing officer may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the officer to do one or more of the following:
>
> (a) access data held in, or accessible from, a computer that is on warrant premises;
>
> (b) copy the data to a data storage device;
>
> (c) convert the data into documentary form.
>
> (2) The magistrate may grant the order if the magistrate is satisfied that:
>
> (a) there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer; and
>
> (b) the specified person is:
>
> (i) reasonably suspected of having committed the offence stated in the relevant warrant; or
>
> (ii) the owner or lessee of the computer; or
>
> (iii) an employee of the owner or lessee of the computer; and
>
> (c) the specified person has relevant knowledge of:
>
> (i) the computer or a computer network of which the computer forms a part; or
>
> (ii) measures applied to protect data held in, or accessible from, the computer.

Puertas, Derecho de las Telecomunicaciones, S. 160 f. Anscheinend geht es aber in der praktischen Anwendung eher darum, im konkreten Einzelfall Informationen über ein bestimmtes Verschlüsselungsverfahren zu erlagen als präventiv alle Schlüssel hinterlegen zu lassen. Der Wortlaut der Norm würde aber auch letzteres zulassen.

402 Crimes Act 1914, Act No. 12, 1914, in der Fassung vom 09.08.2009, verfügbar unter: http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/8F4CE1CECF754A99CA2575F500347BD2/$file/CrimesAct1914Vol1_WD02.pdf (28.10.2009). Eine parallele Vorschrift wurde zugleich auch als `section 201A´ in den `Customs Act 1901´ eingefügt; vgl. den Cybercrime Act 2001, der die Normen einfügte, unter: http://www.comlaw.gov.au/comlaw/Legislation/ActCompilation1.nsf/0/78F3C45ABCF46F42CA256F7100560110/$file/Cybercrime2001.pdf (28.10.2009).

(3) A person commits an offence if the person fails to comply with the order.

Penalty: 6 months imprisonment."

Darauf, ob der Herausgabepflichtige die Daten selbst entschlüsselt und herausgibt oder ob er Passwort oder Schlüssel nennt und die Beamten die Daten entschlüsseln, scheint es meist nicht anzukommen.[403] Eine derartige Herausgabe- bzw. Entschlüsselungspflicht existiert auch in Belgien, Frankreich, Irland,[404] den Niederlanden, dem Vereinigten Königreich, Indien, Malaysia, Singapur sowie Trinidad und Tobago.[405] Zum Teil trifft die Pflicht auch Beschuldigte und Aussageverweigerungsberechtigte (in Australien, Belgien,[406] Frankreich, Irland, dem Vereinigten Königreich,[407] Singapur, Indien, Malaysia sowie Trinidad und Tobago). Die Strafen bei Nichtbefolgung der Herausgabe- bzw. Entschlüsselungspflicht liegen meist zwischen drei Monaten und zwei Jahren Haft (Australien, Belgien, Niederlande, Vereinigtes Königreich, Trinidad und Tobago), teilweise bei bis zu drei Jahren Haft (Frankreich, Malaysia, Singapur) und in Indien sogar bei bis zu sieben Jahren Haft.

IV. Verzicht auf Verschlüsselungsregelungen

Letzte Option des staatlichen Umgangs mit Verschlüsselungsverfahren ist, die Verwendung[408] von Verschlüsselungsverfahren keinerlei innerstaatlichen Beschränkungen zu unterwerfen. Dies ist derzeit die Rechtslage in Deutschland.

Auch hier kann aber diskutiert werden, ob eine derartige staatliche Zurückhaltung aus grundrechtlicher Sicht ausreichend ist: Traten in den bisher vorgestellten Szenarien staatliche Aufgabenerfüllung und Verschlüsselungstechnologien miteinander in Konflikt im Sinne einer (IT-)Sicherheit *vor* dem Staat, ist im Folgenden auch an den Aspekt der IT-Sicherheit *durch* den Staat zu denken:

403 So auch Koops, Crypto Law Survey (Stand 01.07.2008), verfügbar unter: http://rechten.uvt.nl /koops/cryptolaw/cls2.htm (23.10.2009); *Diehl,* DuD 2008, 243, 244.

404 In Irland besteht nur eine Verpflichtung, selbst zu entschlüsseln, aber keine Herausgabepflicht für Schlüssel oder Passwörter; siehe Koops, Crypto Law Survey (Stand 01.07.2008), verfügbar unter: http://rechten.uvt.nl/koops/cryptolaw/cls2.htm (23.10.2009).

405 Ausführliche Informationen bei Koops, Crypto Law Survey (Stand 01.07.2008), verfügbar unter: http://rechte n.uvt.nl/koops/cryptolaw/cls2.htm (23.10.2009).

406 Belgien verpflichtet Beschuldigte und Aussageverweigerungsberechtigte aber nur dazu, Informationen zur Entschlüsselung (also Passwörter und Schlüssel) herauszugeben, und nicht dazu, die Informationen selbst zu entschlüsseln. Hier findet im Hinblick auf das Verbot des Selbstbelastungszwangs also doch eine Unterscheidung statt. Einzelheiten dazu bei Koops, Crypto Law Survey (Stand 01.07.2008), verfügbar unter: http://rechten.uvt.nl/koops/cryptola w/cls2.htm (23.10.2009).

407 So laut Koops, Crypto Law Survey (Stand 01.07.2008), verfügbar unter: http://rechten.uvt.nl/ koops/cryptolaw/cls2.htm (23.10.2009) jedenfalls die Rechtsprechung.

408 Import und Export von Verschlüsselungsverfahren und Verschlüsselungsprodukten sind nicht Gegenstand dieser Betrachtung, da derartige Restriktionen allenfalls mittelbar der Aufrechterhaltung staatlicher Kenntnisnahmemöglichkeiten dienen.

Der Staat selbst erhebt, speichert und verwaltet riesige Menge an Daten der Grundrechtsberechtigten. Diese Informationen werden zunehmend digital gespeichert bzw. übermittelt. Mit der steigenden Verbreitung von E-Government- und E-Justice-Angeboten kommuniziert der Staat außerdem nicht nur immer mehr auf digitalem Weg mit dem Einzelnen, auch der behördeninterne *`workflow´* bewegt sich weg von der Akte in Papierform und verlagert sich in verwaltungseigene Intranets. Dabei stellt sich die Frage, ob und welche Qualität an IT-Sicherheit der Staat gewährleisten muss, um die Daten vor Angriffen (Kenntnisnahme, Manipulation etc.) Dritter zu schützen. Im Hinblick auf Verschlüsselung reduziert sich dies auf die Frage, ob der Staat auf den Einsatz von Verschlüsselung verzichten kann (Teil 6):

Szenario 4 (unmittelbare Schutzpflicht)
Staat S verschlüsselt Daten nicht.

Darüber hinaus könnte es auch geboten sein, Private zum Einsatz von Verschlüsselungsverfahren zu verpflichten (Teil 6):

Szenario 5 (mittelbare Schutzpflicht)
Staat S verpflichtet Dritte nicht dazu, Daten zu verschlüsseln.

C. Grundrecht auf Verschlüsselung? – Dimensionen und Strukturierung der weiteren Prüfung

Verschlüsselungsverfahren werden von den unterschiedlichsten Akteuren (private Nutzer, Unternehmen, Berufsgeheimnisträger, Kriminelle, staatliche Stellen etc.) zur Verwirklichung verschiedener Ziele (Vertraulichkeit, Integrität, Authentizität, Zurechenbarkeit, Anonymität) eingesetzt. Auch wenn im Kern jeweils Verschlüsselungsverfahren eingesetzt werden, unterscheiden sich die verwendeten Techniken: Verschlüsselung, digitale Signatur, Anonymisierungsdienste etc. Schließlich differieren auch die dahinter stehenden Motive: Schutz der Privatsphäre, wirtschaftliche oder wissenschaftliche Motive usw. Verschlüsselung spielt überall da eine Rolle, wo Informationen in Form von Daten vorliegen; mit der zunehmend allumfassenden Digitalisierung betrifft Verschlüsselung nahezu alle Lebensbereiche. Daher sind nicht nur unterschiedliche Akteure, Schutzziele, Techniken und Motive, sondern auch eine Vielzahl von Grundrechten (möglicherweise) betroffen.

Innerhalb der grundrechtlichen Perspektive kann schließlich noch weiter differenziert werden nach den verschiedenen Grundrechtsdimensionen:

- Von einem „Grundrecht auf“ ein bestimmtes Verhalten kann zunächst gesprochen werden, wenn ein Verbot dieses Verhaltens nicht in grundrechtskonformer Weise möglich ist. [409] Damit ist die klassische,[410] abwehrrechtliche Dimension von Grundrechten angesprochen: Ein bestimmtes Verhalten fällt in den Schutz-

409 *Murswieck*, in: *Sachs,* GG, Art. 2, Rn. 22.
410 *Dreier*, in: *Dreier,* GG, Vorbemerkung, Rn. 85.

bereich eines oder mehrerer Grundrechte und der durch das Verbot bewirkte Eingriff ist verfassungsrechtlich nicht zu rechtfertigen.

- Ein demgegenüber „qualifiziertes“ „Grundrecht auf“ liegt vor, wenn auch eine Grundgesetzänderung mit dem Ziel, das betreffende Verhalten zu untersagen oder einzuschränken, nicht in verfassungsgemäßer Weise möglich ist. Dies ist immer dann der Fall, wenn eine solche Änderung den Menschenwürdegehalt (Art. 1 I GG) des betreffenden Grundrechts berührt oder einen sonstigen Verstoß gegen die Ewigkeitsgarantie (Art. 79 III GG) bedeuten würde.
- Neben dieser abwehrrechtlichen Betrachtungsweise kann aber auch dann von einem „Grundrecht auf“ ein bestimmtes Verhalten gesprochen werden, wenn den Staat positive Pflichten aus Grundrechtsnormen treffen, dieses Verhalten zu gewährleisten oder zu fördern. Voraussetzung ist, dass sich aus dem jeweiligen Grundrecht objektiv-rechtliche Gehalte deduzieren lassen, die sich dann zu staatliche Schutzpflichten, Anforderungen an staatliche Verfahrensgestaltung oder zu Leistungs- und Teilhaberechten verdichten können.

Die vorgestellten Szenarien bieten nicht nur Raum, die (teils übereinstimmenden, teils divergierenden) Interessen der verschiedenen Akteure und die differierenden Zielsetzungen zu erörtern, sie bilden auch die angesprochenen Grundrechtsdimensionen ab:

Zunächst werden die Grenzen staatlicher Regulierungsoptionen erörtert, ausgehend vom stärksten denkbaren Eingriff, einem staatlichen Verbot von Verschlüsselung (Teil 3). Ist ein Verbot verfassungsrechtlich zu rechtfertigen, erübrigt sich ein Nachdenken über Implikationen objektiv-rechtlicher Grundrechtsgehalte. Andernfalls sind in einem nächsten Schritt sonstige Reglementierungsmöglichkeiten grundrechtlich zu untersuchen, und zwar zunächst relative Verschlüsselungsverbote (Teil 4) sowie im Anschluss gesetzliche Herausgabepflichten (Teil 5). Nachdem so die Grenzen staatlicher Regelungsmöglichkeiten konturiert sind, soll anhand mehrerer Szenarien untersucht werden, ob sich positive Forderungen nach einem „Recht auf Verschlüsselung“ aus Grundrechten ergeben und welche dies im Einzelnen sind (Teil 6).

Teil 3: Grundrecht auf Verschlüsselung im Kontext eines absoluten Verschlüsselungsverbots

Die denkbar restriktivste Form des staatlichen Umgangs mit Verschlüsselungstechnologien ist ein umfassendes Verbot von Verschlüsselungsverfahren. Ein solches Verbot existiert derzeit in der Bundesrepublik nicht. Trotzdem ist das

Szenario 1
Staat S verbietet Verschlüsselungsverfahren.

nicht nur eine rein hypothetische Option:

Weltweit gibt es derzeit einige Staaten, die versuchen, durch ein umfassendes Verbot oder eine einem Verbot gleichkommende Genehmigungspflicht Kenntnisnahmeoptionen staatlicher Sicherheitsbehörden sicherzustellen.[411] Auch wenn die Liste der Staaten mit einem absoluten Verschlüsselungsverbot bzw. einer staatlichen Genehmigungspflicht vor allem nicht-demokratische Staaten sowie postkommunistische Staaten des ehemaligen Ostblocks, die sich in einem noch andauernden Demokratisierungsprozess befinden, umfasst, darf ein absolutes Verschlüsselungsverbot nicht als für gefestigt demokratische Staaten irrelevantes Modell abgetan werden: Bis zum Jahr 1996 unterlag die Verwendung von Verschlüsselungsverfahren zum Schutz der Vertraulichkeit auch in Frankreich einer Genehmigungspflicht.[412] 1994 sollte in den Niederlanden eine Genehmigungspflicht eingeführt werden.[413]

Auch in Deutschland fand Mitte der Neunziger Jahre eine so genannte Kryptokontroverse statt.[414] Die restriktive Regulierung der Nutzung von Verschlüsselungsverfahren wurde etwa vom damaligen Innenminister Manfred Kanther gefordert[415] und auf politischer wie juristischer Ebene diskutiert.[416] Erst das Eckwertepapier der

411 S.o. in Teil 2 unter B.I.

412 *Kuner*, in: *Hoeren/Sieber,* Handbuch Multimedia-Recht, Teil 17, Rn. 76 ff; Koops, Crypto Law Survey (Stand 01.07.2008), verfügbar unter: http://rechten.uvt.nl/koops/cryptolaw/cls2.htm (23.10.2009).

413 *Kuner*, in: *Hoeren/Sieber,* Handbuch Multimedia-Recht, Teil 17, Rn. 97; *Koops*, The crypto controversy, S. 125.

414 Diese drehte sich zwar hauptsächlich um Szenarien, die als relative Verschlüsselungsverbote (siehe dazu Szenario 2 in Teil 4) zu qualifizieren sind. Die Option eines absoluten Verschlüsselungsverbots war aber ebenfalls Bestandteil der Debatte (vergleiche etwa die damalige Stellungnahme der FDP, die explizit diese Möglichkeit erwähnte, zitiert bei *Andrzejak*, Kryptoregulierung, in: *Hoeren/Queck,* Rechtsfragen der Informationsgesellschaft, S. 132, 138).

415 Siehe die Rede von Bundesinnenminister Manfred Kanther anlässlich der Eröffnung des 5. IT-Sicherheitskongresses am 28. April 1997 in Bonn, verfügbar unter: http://www.iks-jena.de/mitarb/lutz/security/cryptoban/kanther.rede.html (15.09.2008).

416 Diskutiert wurde vor allem eine generelle Genehmigungspflicht unter strafbewehrtem Verbot der Nutzung nicht genehmigter Verfahren; siehe zu den Positionen *Andrzejak*, Kryptoregulierung, in: *Hoeren/Queck,* Rechtsfragen der Informationsgesellschaft, S. 132, 137 ff.

Bundesregierung zur Kryptopolitik vom 02.06.1999[417] beendete die Debatte mit der politischen Entscheidung, die Verwendung von Verschlüsselungsverfahren einstweilen nicht zu beschränken. Das Eckwertepapier war zwar rechtlich nicht bindend, da es sich nur um eine Absichtserklärung der damaligen Bundesregierung handelt; rechtspolitisch war die im Eckwertepapier niedergelegte Entscheidung der Bundesregierung, die Nutzung von Verschlüsselungsverfahren nicht zu beschränken, aber höchst bedeutsam. Dies zeigt sich nicht zuletzt daran, dass bis heute an der im Eckwertepapier festgelegten Grundsatzentscheidung festgehalten wurde.

Das Szenario eines absoluten Verschlüsselungsverbots ist also durchaus praktisch relevant. Dies gilt nicht nur für die – als autoritär kategorisierbaren – Staaten, in denen derzeit ein absolutes Verschlüsselungsverbot gilt. Es ist noch nicht lange her, dass auch westliche Demokratien absolute Verschlüsselungsverbote erlassen haben.

Eine grundrechtliche Prüfung absoluter Verschlüsselungsverbote ist darüber hinaus im Sinne einer Abschichtung der verfassungsrechtlichen Fragestellungen sinnvoll. Es gilt zunächst grundlegend zu untersuchen, ob und wenn gegen welche Grundrechte ein absolutes Verschlüsselungsverbot verstoßen würde. Die Besonderheiten eines weniger eingriffsintensiven relativen Verschlüsselungsverbots in seinen verschiedenen Varianten (von der Zulassung nur kurzer Schlüssellängen über Verfahren mit technischer Hintertür bis zu Schlüsselhinterlegungs- und Nachschlüsselmodellen[418]) erfolgt dann in einem gesonderten Teil 4. Absolute und relative Verschlüsselungsverbote haben gemeinsam, dass die Nutzung von Verschlüsselungsverfahren (ganz oder teilweise) beschränkt wird. Die grundrechtliche Prüfung erfolgt insoweit parallel. Im Hinblick auf die Komplexität der Materie (mögliche Betroffenheit einer Vielzahl von Grundrechten, multiple Akteure, verschiedenartige Interessen und Motive etc.) erscheint es sinnvoll, zunächst in einem „clear case"-Szenario die Verfassungsmäßigkeit eines absoluten Verschlüsselungsverbots zu prüfen und eine grundlegende Strukturierung und rechtliche Einordnung zu leisten. Sodann kann in einem „hard case"-Szenario auf die Besonderheiten der einzelnen Modelle eines relativen Verschlüsselungsverbots eingegangen werden.

A. Verschlüsselungsverbot und Privatsphärenschutz

Hinsichtlich der Verfassungsmäßigkeit absoluter Verschlüsselungsverbote können grundsätzlich zwei Perspektiven unterschieden werden, die sich aus den betroffenen Akteuren und Interessen ergeben. Zum einen die Perspektive der (potentiellen) Verwender von Verschlüsselungsprodukten. Privatpersonen, Unternehmen und auch den Staat selbst verbindet hier die Verfolgung ihrer jeweiligen Geheimhaltungsinte-

417 Siehe Bundesministerium des Innern, Pressemitteilung vom 02.06.1999, verfügbar unter: http ://www.bmi.bund.de/cln_028/nn_678294/Internet/Content/Nachrichten/Archiv/Pressemitteilungen/1999/06/Eckpunkte__der__deutschen__Kryptopolitik__Id__26320__de.html (04. 07. 2008)

418 Siehe ausführlich dazu in Teil 4.

ressen. Hier kann weiter unterschieden werden zwischen dem Schutz privater Geheimnisse und dem Schutz sonstiger (zumeist kommerzieller) Geheimnisse. Diese zweite Perspektive, bei der es hauptsächlich um die Realisierung der wirtschaftlichen Betätigungsfreiheit geht, ist zugleich die der Hersteller von Verschlüsselungsprodukten, die sich im Falle eines absoluten Verschlüsselungsverbots ihres Geschäftsfeldes beraubt sehen (dazu unter B.)

Ein absolutes Verbot von Verschlüsselungsverfahren hätte für jedermann die folgenden Konsequenzen:

- E-Mails und andere Daten könnten nur unverschlüsselt und damit für jedermann lesbar[419] versendet werden.
- E-Mails und andere Daten könnten nicht signiert und damit leicht unbemerkt verändert[420] werden.
- Anonyme Internetnutzung wäre nicht möglich, der Internetanschluss wäre stets feststellbar[421] und damit prinzipiell auch die dahinter stehende Person.
- Daten dürften nicht verschlüsselt gespeichert werden, so dass jeder, der Zugang zum Speichermedium hat, die Daten auch inhaltlich zur Kenntnis nehmen könnte.[422]

Für Privatpersonen steht damit eine Betroffenheit ihrer „Privatsphärengrundrechte“ im Raum. Unter diesen Begriff werden traditionellerweise[423] das Brief-, Post- und Fernmeldegeheimnis (Art. 10 I GG; dazu I.), das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 I GG; dazu II.) sowie das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG; dazu III.), insbesondere in seinen Ausprägungen als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und als Recht auf informationelle Selbstbestimmung subsumiert.

I. Verstoß gegen das Brief-, Post- und Fernmeldegeheimnis (Art. 10 I GG)

Brief-, Post- und Fernmeldegeheimnis schützen die Vertraulichkeit individueller Kommunikation, soweit diese wegen der räumlichen Distanz der Beteiligten auf einen Übermittler angewiesen ist.[424] Brief-, Post- und Fernmeldegeheimnis wollen einen adäquaten rechtlichen Schutz bieten als Ausgleich für die besonderen Übermittlungsgefahren:[425] Aus der notwendigen Einschaltung eines Übermittlers resultieren besondere Zugriffsmöglichkeiten, zum einen für den Übermittler selbst, zum ande-

419 S.o. in Teil 1 unter B.I.b.aa).
420 S.o. in Teil 1 unter B.II.1.
421 S.o. in Teil 1 unter B.I.1.c.
422 S.o. in Teil 1 unter B.II.1.b.
423 *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 2.
424 *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 15.
425 Zur technischen und einfachgesetzlichen Situation bei Datenkommunikation siehe oben in Teil 1 unter B.I. und C.II.

ren (regelmäßig über den Übermittler) für staatliche Stellen und nicht zuletzt für unbefugte Dritte. Art. 10 I GG gewährleistet insoweit eine „Privatheit auf Distanz“.[426]

1. Schutzbereich des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 I GG)

Der Schutzbereich des Art. 10 I GG müsste die Verwendung von Verschlüsselungsverfahren umfassen. Dabei können zwei Aspekte unterschieden werden: Zum einen ist in einer inhaltlichen Perspektive zu untersuchen, ob Kommunikation mittels verschlüsselter Daten vom Schutzbereich umfasst ist. In einer prozeduralen Perspektive stellt sich die Frage, ob auch der Einsatz von Verschlüsselungsverfahren zur Generierung der verschlüsselten Daten vom Schutzbereich des Art. 10 I GG umfasst ist.

a. Verschlüsselte Daten im Schutzbereich des Art. 10 I GG

Zweifelsohne liegen jeder elektronischen Kommunikation, Internetnutzung oder jeder sonstigen Nutzung von Informations- und Kommunikationstechnologien „Daten“ zugrunde. Der Schutzbereich des Art. 10 I GG erfasst auch diese modernen Kommunikationsformen. Daten sind nach der DIN-Norm 443000 definiert als

> „Gebilde aus Zeichen oder kontinuierliche Funktionen, die aufgrund bekannter oder unterstellter Abmachungen Informationen darstellen.“[427]

Danach beinhaltet der Datenbegriff nicht nur digitale, sondern auch analoge Daten. Jegliche Art codierter Information stellt ein Datum im informationstechnischen Sinn dar.[428] Bereits die Schriftzeichen eines handgeschriebenen Briefes stellen (analoge) Zeichen dar, die aufgrund von Abmachungen Informationen vermitteln. Zu prüfen bleibt, welches der drei Grundrechte[429] des Art. 10 I GG bzw. welche der drei Grundrechtsgarantien[430] für den Schutz von Datenübermittlungen maßgeblich ist.

426 *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 19.

427 DIN-Norm 443000, zitiert nach *Kloepfer,* Informationsrecht, § 1, Rn. 58.

428 Zu Begriff und Differenzierung von Information und Datum siehe auch *Zöller*, Allgemeine Grundsätze bei Datenübermittlungen von Sicherheitsbehörden, in: *Roggan/Kutscha,* Handbuch zum Recht der Inneren Sicherheit, S. 448, 448 f.

429 Für die Qualifizierung von Brief-, Post- und Fernmeldegeheimnis als drei selbständige Grundrechte sprechen sich etwa *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 25 und *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 25 aus.

430 Dagegen sieht etwa *Jarass/Pieroth,* GG, Art. 10, Rn. 1 ff. in Art. 10 I GG ein einheitliches Grundrecht mit drei Teilgarantien. Da dies in der Sache aber keinerlei Konsequenzen mit sich bringt, kann die Frage dahinstehen.

aa) Briefgeheimnis

Insbesondere für E-Mails, die vielfach als „elektronische Post" bezeichnet werden, drängt sich der Gedanke auf, dass es sich um „Briefe" handeln könnte. Nach einer Kommentarmeinung sind Briefe im Sinne des Art. 10 I GG

> „alle den mündlichen Verkehr ersetzenden, an einen individuellen Empfänger gerichteten, schriftlich fixierten Nachrichten, Gedanken und Meinungen […]."[431]

Fraglich ist danach allein, ob E-Mails in diesem Sinne als „schriftlich fixiert" angesehen werden können. Denkbar wäre, im Wege der teleologischen Auslegung angesichts der technischen Entwicklung die digitale Speicherung als Fixierung ausreichen zu lassen. Dann wäre allein die Frage, ob E-Mails das Schriftlichkeitskriterium erfüllen, entscheidend. Für die „Schriftlichkeit" von E-Mails spricht, dass sich eine ausgedruckte E-Mail durch nichts von einem traditionellen Brief unterscheidet. Es handelt sich jeweils um ein Blatt Papier, auf dem sich Schriftzeichen befinden. Auch in digitaler Form scheint eine E-Mail aus Schriftzeichen zu bestehen, die über einen Bildschirm oder ein Display sichtbar gemacht werden. Tatsächlich handelt es sich aber schlicht um digitale Daten. Charakteristikum digitaler Daten ist, dass sie nicht körperlich,[432] und damit per se auch nicht schriftlich sind. Die Darstellung der in den Daten enthaltenen Informationen durch Schriftzeichen ist eine *Form* der Darstellung der Daten. Es handelt sich nicht um die Daten selbst. E-Mails erfüllen daher nicht das Kriterium der „Schriftlichkeit". Soweit zur Abgrenzung auf das Erfordernis der Körperlichkeit des „Briefs" abgestellt wird,[433] ergibt sich nichts anderes.

Daten und insbesondere E-Mails fallen daher nicht in den Schutzbereich des Briefgeheimnisses. Dem steht auch nicht der häufig zu findende Vergleich[434] von E-Mails mit Postkarten entgegen. Dieser bezieht sich vor allem auf die Möglichkeit der inhaltlichen Kenntnisnahme durch beliebige Dritte bei der Übermittlung, und nicht auf die Qualifizierung einer E-Mail als „Brief" oder Postsendung im Sinne des Art. 10 I GG.[435]

431 *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 30.

432 Insoweit weiter differenzierend *Störing*, Strafprozessuale Zugriffsmöglichkeiten auf E-Mail-Kommunikation, S. 25, der betont, dass die per se nicht-körperlichen Informationen grundsätzlich an einen physischen Datenträger gebunden sind. Sodann stellt *Störing* aber vorwiegend auf den nicht-körperlichen Transportweg ab und hält im Ergebnis ebenfalls das Fernmeldegeheimnis für einschlägig.

433 Vergleiche etwa *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 27; *Möller,* DuD 2000, 267, 269; *Störing*, Strafprozessuale Zugriffsmöglichkeiten auf E-Mail-Kommunikation, S. 35.

434 Vgl. *Brüning/Helios,* Jura 2001, 155, 156: „Innerhalb des Netzes bestehen keine Schutzmechanismen, die einen unbefugten Zugriff zumindest erschweren. Die eMail gleicht insoweit einer für jeden lesbaren Postkarte." sowie Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung, Bürgerportale, verfügbar unter: http://www.kbst.bund.de/nn_836958/Content/Egov/Bportale/bportale.html__nnn=true (19.09. 2008).

435 Für diese Einschätzung spricht etwa das Urteil des LG Köln vom 28.05.2008, Az.: 28 O 157/08, Rn. 29 (juris), das den Postkartenvergleich ablehnt und wegen der nicht verlassenen Geheimsphäre eine Parallele zu einem verschlossenen Brief zeiht.

bb) Fernmeldegeheimnis

Die Eröffnung des Schutzbereichs des Fernmeldegeheimnisses setzt zum einen den Einsatz nicht-körperlicher Übermittlungstechnologien voraus und zum anderen das Vorliegen von Individualkommunikation.

(1) Nicht-körperliche Übermittlung

Das Fernmeldegeheimnis schützt als Zusammenfassung des früheren „Telegraphen- und Fernsprechgeheimnisses" des Art. 117 der Weimarer Reichsverfassung (WRV) die gesamte nicht-körperliche Übermittlung von Information. Es umfasst nach der Rechtsprechung des BVerfG

> „[…] sämtliche mit Hilfe der verfügbaren Telekommunikationstechniken erfolgenden Übermittlungen von Informationen. Auf die konkrete Übermittlungsart (etwa über Kabel oder Funk, durch analoge oder digitale Vermittlung) und Ausdrucksform (etwa Sprache, Bilder, Töne, Zeichen oder sonstige Daten) kommt es nicht an."[436]

Dieser weiten Definition des Fernmeldegeheimnisses entspricht, dass der Fernmeldebegriff bewusst offen konzipiert wurde.[437] Danach unterliegen sämtliche mittels Telekommunikation übermittelten Daten dem Schutz des Fernmeldegeheimnisses, also neben herkömmlichen Telefonaten auch E-Mails oder Internettelefonie.[438] Neben dem Kommunikationsinhalt wird auch der Kommunikationsvorgang geschützt.[439] Auch die näheren Umstände der Telekommunikation wie die beteiligten Anschlüsse und Personen, Zeitpunkt und Dauer von Telekommunikationsverbindungen und –verbindungsversuchen unterfallen somit dem Schutz des Fernmeldegeheimnisses.[440]

436 BVerfG, Beschluss vom 09.10.2002, Az.: 1 BvR 1611/96 und 805/98, Rn. 19.

437 So *Hadamek*, Art. 10 GG und die Privatisierung der Deutschen Bundespost, S. 216 unter Verweis auf BVerfGE 46, 120, 143 – Direktrufverordnung; *Kloepfer,* Informationsrecht, § 3, Rn. 32.

438 So ausdrücklich BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 43: „Die Reichweite des Grundrechts erstreckt sich […] auch auf Kommunikationsdienste des Internet." sowie BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 192: „Insbesondere gilt dies auch für die Speicherung der Daten zu Diensten der elektronischen Post gemäß § 113a Abs. 3 TKG, deren Vertraulichkeit gleichfalls durch Art. 10 Abs. 1 GG geschützt wird."

439 *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 40 f.; *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 45.

440 *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 41; *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 45; *Störing*, Strafprozessuale Zugriffsmöglichkeiten auf E-Mail-Kommunikation, S. 32.

(2) Individualkommunikation

Es muss sich grundsätzlich um Individualkommunikation handeln und nicht um Inhalte, die sich an die Allgemeinheit richten.[441] Dann würde es sich um Rundfunk[442] oder (elektronische) Presse[443] handeln. Allerdings bereitet die Abgrenzung von Individual- und Massenkommunikation angesichts der zunehmenden Konvergenz der Medien und Dienste einige Schwierigkeiten.[444] Entscheidendes Abgrenzungskriterium dürfte die öffentliche Zugänglichkeit von Massenkommunikation im Gegensatz zu im Wege besonderer Sicherungen geschützter Individualkommunikation sein.[445] Den übertragenen Daten selbst ist aber ohne Kenntnisnahme des Inhalts oder der näheren Umstände der Kommunikation nicht anzusehen, ob es sich um Individual- oder Massenkommunikation handelt. In dieser Situation muss es für die Eröffnung des Schutzbereichs des Fernmeldegeheimnisses ausreichen, dass die *Möglichkeit* besteht, dass es sich um geschützte Individualkommunikation handelt:[446]

> „Sofern auf diese Weise wegen der technischen Gegebenheiten keine Abgrenzung möglich ist, bleibt es dabei: In solchen Fällen muss für den Grundrechtsschutz des Art. 10 Abs. 1 die Möglichkeit genügen, dass mit einem elektronischen Medium auch Individualkommunikation vermittelt wird. Das gilt insbesondere, wenn die Abgrenzung allein durch die Kenntnisnahme grundrechtlich geschützter Information möglich ist.“[447]

Nach diesem Gedanken der Formalisierung des Schutzes muss der Schutz der Übermittlung von Daten im Wege der Telekommunikation umfassend sein und alle Formen der Datenübermittlung und Kommunikation beinhalten:[448]

441 *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 42. Der Amateurfunk, für den ein einfachgesetzliches Verschlüsselungsverbot besteht (siehe oben in Teil 1 unter C.III.) fällt daher per definitionem (§ 2 Nr. 2 AmateurfunkG) nicht in den Schutzbereich des Fernmeldegeheimnisses, da Amateurfunk stets an die Allgemeinheit gerichtet ist.

442 *Dill*, Rundfunkbegriff und Telekommunikationsdienste, in: *Haratsch/Kugelmann/Repkewitz,* Herausforderungen an das Recht der Informationsgesellschaft, S. 81; *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 42; *Schulze-Fielitz*, in: *Dreier,* GG, Art. 5 I, II, Rn. 99 ff.

443 *Grote,* KritV 1999, 27, 37, der daneben aber auch noch andere möglicherweise einschlägigen Medienfreiheiten erörtert und versucht, die verschiedenen Internet-Kommunikationsdienste zuzuordnen, vgl. ebd. S. 32 ff.

444 Dazu *Schoch*, Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57, 158, 170 f. m.w.N.

445 *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 43; *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 39; *Löwer*, in: *v. Münch/Kunig,* GG, Art. 10, Rn. 18; *Valerius*, Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet, S. 71 ff.

446 *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 39; *Störing*, Strafprozessuale Zugriffsmöglichkeiten auf E-Mail-Kommunikation, S. 31; v. *Bonin*, Die Kontrolle digitaler Kommunikationsinhalte, S. 106.

447 *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 44.

448 Das BVerfG sieht auch in der Speicherung der den Internetzugang als solchen betreffenden Daten (Vorratsdatenspeicherung nach §§ 113a, b TKG) einen Eingriff in Art. 10 I GG: „Da eine Unterscheidung zwischen Individual- und Massenkommunikation ohne eine der Schutzfunktion des Grundrechts zuwiderlaufende Anknüpfung an den Inhalt der jeweils übermittelten Information nicht möglich ist, ist bereits in der Speicherung der den Internetzugang als

„Während nach traditioneller Auffassung nur der Austausch von Nachrichten, Gedanken und Meinungen (Informationen) den grundrechtlichen Schutz genießen soll, müssen angesichts der technischen Untrennbarkeit des Übermittlungsvorgangs auch Bilder, Zeichen und jede Art sonstiger Daten in den Schutzbereich von Art. 10 GG fallen. Deshalb genießen nicht nur die traditionellen Sprachübermittlungsdienste in geschäftlicher wie privater Nutzung, sondern auch alle anderen Formen individueller Datenübermittlung den grundrechtlichen Schutz des Fernmeldegeheimnisses und damit auch jede elektronische Kommunikationsform durch das Internet."[449]

(3) Fehlende Schutzbedürftigkeit verschlüsselter Daten?

Angesichts dieses weiten Schutzbereichs liegt der Gedanke nahe, dass auch die Übermittlung verschlüsselter Daten von diesem umfasst ist. Gegen eine Eröffnung des Schutzbereichs könnte allerdings sprechen, dass Daten, die mit Hilfe von starken Verschlüsselungsverfahren verschlüsselt wurden, überhaupt nicht den spezifischen, aus der notwendigen Inanspruchnahme eines Kommunikationsmittlers resultierenden Kenntnisnahmegefahren ausgesetzt sind. Diese Gefahren stellen nach dem BVerfG Grundlage und materielle Rechtfertigung der Grundrechte des Art. 10 GG dar:

„Brief-, Post- und Fernmeldegeheimnis gewährleisten die Vertraulichkeit der individuellen Kommunikation, wenn diese wegen der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch andere angewiesen ist und deshalb in besonderer Weise einen Zugriff Dritter – einschließlich staatlicher Stellen – ermöglicht."[450]

Die Vertraulichkeit der räumlich distanzierten Individualkommunikation wird – so könnte man in teleologischer Auslegung demnach formulieren – grundrechtlich gewährleistet, (gerade) weil und (nur) soweit durch die Übermittlung in besonderer Weise die Kenntnisnahme Dritter ermöglicht wird.

Gegen diese Argumentation spricht grundsätzlich, dass es bei der Bestimmung des Schutzbereichs eines Grundrechts zunächst nur um „die Feststellung der Einschlägigkeit einer Grundrechtsnorm in sachlicher und personeller Hinsicht"[451] geht. Im Sinne größerer dogmatischer Klarheit sollten daher eingriffs- oder schrankenorientierte Interpretationen bei der Schutzbereichsbestimmung nicht vorweg genommen werden. Aus der technischen Sicherung gegen unbefugte Kenntnisnahme kann daher keine Reduktion des Schutzbereichs des Fernmeldegeheimnisses abgeleitet werden.

solchen betreffenden Daten ein Eingriff zu sehen, auch wenn sie Angaben über die aufgerufenen Internetseiten nicht enthalten."; BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 192.

449 *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 40.

450 BVerfG, Urteil vom 02.03.2006, Az.: 2 BvR 2099/04, Rn. 65.

451 *Dreier*, in: *Dreier,* GG, Vorbemerkung, Rn. 120.

(4) Gleichbehandlung verschlüsselter Daten mit unverschlüsselten Daten

Für eine Erfassung verschlüsselter Daten vom Schutzbereich des Fernmeldegeheimnisses sprechen vielmehr folgende sieben Argumente:

(a) Ununterscheidbarkeit von verschlüsselten und unverschlüsselten Daten

Zum einen unterscheiden sich verschlüsselte Daten nicht von unverschlüsselten.[452] Eine Anforderung, dass die durch Art. 10 GG geschützten Daten sinnvoll oder allgemein verständlich sein müssten, existiert nicht. Bei näherer Betrachtung erweist sich zudem jede Kommunikation in gewissem Sinn als „verschlüsselt", da sie immer eine irgendwie geartete Codierung erfordert – sei es durch die Verwendung von Sprache, Signalen, Zeichen oder ähnlichem.[453]

(b) Fortbestehender Vertraulichkeitsbedarf

Zweitens besteht auch bei Einsatz von Verschlüsselungsverfahren ein Vertraulichkeitsbedarf fort. Das Fernmeldegeheimnis schützt neben der Vertraulichkeit des Kommunikationsinhalts auch die Vertraulichkeit der näheren Umstände der Kommunikation.[454] Zwar können Verschlüsselungsverfahren die Vertraulichkeit von Inhalten *und* Umständen sichern, dazu sind aber – technisch – zwei *verschiedene* Vorgehensweisen erforderlich.[455] Die technisch getrennten Vorgänge sind daher auch zunächst getrennt zu analysieren. Wird der Kommunikationsinhalt verschlüsselt, erfasst dies nicht auch die Kommunikationsumstände: Bei einer E-Mail wird etwa nur der *`body´* mit dem Inhalt der Nachricht verschlüsselt, der *`header´* der E-Mail bleibt unverschlüsselt, da er für die bestimmungsgemäße Übermittlung maßgeblich ist. Die Kommunikationsumstände bleiben also ungeschützt, obwohl sie gleichermaßen in den Schutzbereich von Art. 10 I GG fallen. Daher bleibt auch bei verschlüsselten E-Mails ein nicht technisch gedeckter Vertraulichkeitsbedarf, nämlich hinsichtlich der Kommunikationsumstände.

Im umgekehrten Fall gilt das Gleiche: Werden nicht verschlüsselte Inhalte etwa mit Hilfe eines Anonymisierungsdienstes versandt, sind zwar – unter anderem durch den Einsatz von Verschlüsselungsverfahren – die Kommunikationsumstände vertraulich, nicht aber die Kommunikationsinhalte. Auch hier verbleibt ein nicht technisch gedeckter Bedarf an rechtlichem Vertraulichkeitsschutz.

452 Ein Bit kann im Binärcode jeweils nur die Zustände 0 oder 1 annehmen. Daraus ergeben sich keine Hinweise darauf, ob die Daten verschlüsselt sind oder nicht. Siehe dazu ausführlich *Meyn*, Verschlüsselung und Innere Sicherheit, S. 54.

453 *Meyn*, Verschlüsselung und Innere Sicherheit, S. 59; zu Sprache als Medium, das Bedeutungen vermittelt siehe *Hartmann*, Sichere Kommunikation im Internet, S. 5.

454 *Löwer*, in: *v. Münch/Kunig,* GG, Art. 10, Rn. 22; *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 45; *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 40, 41.

455 Siehe dazu oben in Teil 1 unter A.IV.1.

(c) Formalisierung des Schutzes

Für eine Eröffnung des Schutzbereichs auch für verschlüsselte Daten spricht weiter der bereits dargestellte Gedanke der Formalisierung des Schutzes. Denn auch hier müssten die Daten erst zur Kenntnis genommen werden, um dann die Beurteilung zu ermöglichen, ob diese (sicher?) verschlüsselt sind oder nicht. Dieses Vorgehen widerspräche aber gerade der Schutzrichtung des Fernmeldegeheimnisses.

(d) Fortdauernde Schutzwürdigkeit verschlüsselter Daten

Durch den Einsatz von Verschlüsselungsverfahren wird im Wege technischer Schutzmaßnahmen genau das erreicht, was das Fernmeldegeheimnis rechtlich gewährleisten will: die Vertraulichkeit der räumlich distanzierten Kommunikation. Daher muss die Nutzung von Verschlüsselungsverfahren in den Schutzbereich des Fernmeldegeheimnisses fallen.[456] *Andernfalls käme man zu dem absurden Ergebnis, dass die effektivste Maßnahme zum Schutz des Fernmeldegeheimnisses nicht vom Schutzbereich des Fernmeldegeheimnisses umfasst wäre.* Die durch das Grundrecht des Art. 10 GG anerkannte Schutzwürdigkeit des Fernmeldegeheimnisses kann nicht durch Maßnahmen gerade zum Schutz des Fernmeldegeheimnisses entfallen:

> "Mit einer derartigen Schutzmöglichkeit wird das Fernmeldegeheimnis wieder auf seinen ursprünglichen Grund zurückgeführt, nämlich ein *individuelles* Schutzrecht gegen staatliche Eingriffe in die Vertraulichkeit der Kommunikation zu sein. Ein Verbot von Kryptoverfahren unter den heutigen Bedingungen der Telekommunikation würde jedoch das Fernmeldegeheimnis just in dem Moment preisgeben, in dem sich die Teilnehmer von den Schutzmöglichkeiten, die die Betreiber von Fernmeldeanlagen anbieten, emanzipieren können."[457]

(e) Fortdauernde Schutzbedürftigkeit verschlüsselter Daten

Trotz des Einsatzes effektiver Selbstschutzmaßnahmen entfällt die Schutzbedürftigkeit der Daten nicht. Auch die Verwendung von Verschlüsselungsverfahren beseitigt nicht alle Vertraulichkeitsrisiken. Auch wenn die Besonderheit von Verschlüsselung als absolut sicherem technischem Verfahren immer wieder hervorgehoben wurde, darf dies nicht den Blick dafür verstellen, dass es gleichwohl eine Vielzahl anderweitiger Möglichkeiten gibt, auf Kommunikationsinhalte zuzugreifen.

Ein technisches Verfahren kann für sich allein noch so sicher sein, es ist stets eingebettet in ein Gesamtkonzept von IT-Sicherheitsmaßnahmen. Bei der Beurteilung eines bestimmten Vorgangs, etwa des Versendens einer verschlüsselten E-Mail, ist

456 So auch *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 186 f.; *Groß,* JZ 1999, 326, 334; *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 50; *Löwer*, in: *v. Münch/Kunig,* GG, Art. 10, Rn. 11; *Marauhn,* KritV 1999, 57, 81; während *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 46 den grundrechtlichen Schutz der Nutzung von Verschlüsselungsverfahren eher im Bereich der Art. 5 und 2 GG gewährleistet zu sehen scheint.

457 *Bizer,* KritJ 1995, 450, 461.

ein ganzes Bündel von Komponenten zu beurteilen, die in diesen Vorgang involviert sind. So kommt es im gewählten Beispiel nicht nur auf die Sicherheit des verwendeten Verschlüsselungsverfahrens, sondern auch auf die Sicherheit der Passphrase, die Sicherung der Passphrase (auf der eigenen Festplatte oder auf einer Smartcard), die Verwendung eines sicheren Kartenlesegerätes usw. an. Die erreichte (Gesamt-)Sicherheit ist nur so stark wie das schwächste Glied der Kette an Komponenten, die einen bestimmten Vorgang ausmachen:

„Security is a chain; it´s only as secure as the weakest link.“[458]

Die Sicherheit des Verschlüsselungsverfahrens allein sagt also noch nichts über die Sicherheit des Kommunikationsvorgangs als Ganzes aus.[459] Dies spricht für ein Fortbestehen der (rechtlichen) Schutzbedürftigkeit.

Auch werden nicht alle Nutzer für jede Kommunikation ein gleich hohes Sicherheitsniveau anstreben. In der Praxis wird vielfach ein abgestuftes Sicherheitskonzept zur Anwendung kommen, das unterschiedliche technische Sicherheitsniveaus für unterschiedliche Vertraulichkeitsstufen vorsieht. [460] Damit ist absehbar, dass ein erheblicher Teil der Datenkommunikation (zur Erhöhung von Schnelligkeit und Bequemlichkeit) nur mit schwächeren Verschlüsselungsverfahren gesichert sein wird.[461] Für diese Daten besteht unverändert auch ein rechtliches Schutzbedürfnis.

(f) Kein Antagonismus von staatlichem Schutz und Selbstschutz

Selbstschutz und staatlich vermittelter Schutz schließen sich nicht per se gegenseitig aus. Das Konzept des Selbstdatenschutzes zur (besseren) Verwirklichung des Schutzes des Rechts auf informationelle Selbstbestimmung belegt dies. Ein Antagonismus von Selbstschutz und staatlichem Schutz findet sich vor allem im Zusammenhang mit dem staatlichen Gewaltmonopol.[462] Die Gewährleistung staatlichen Schutzes korrespondiert insoweit mit einem Verbot der (privaten) Selbsthilfe. Ein echtes Ausschließlichkeitsverhältnis besteht aber auch hier nicht: Zwar wird der Schutz durch

458 *Schneier*, Secrets and Lies, S. xii.

459 So auch *Beutelspacher*, Ist Kryptographie gut - oder zu gut?, in: *Hamm/Möller,* Datenschutz durch Kryptographie, S. 16, 37.

460 Vergleiche etwa die Einstufung von Verschlusssachen in die Kategorien „streng geheim“, „geheim“, „VS - vertraulich“ sowie „VS - Nur für den Dienstgebrauch“, Bundesministerium für Wirtschaft und Arbeit, Handbuch für den Geheimschutz in der Wirtschaft, verfügbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/bmwa-geheimschutzhandbuch,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf (28.06.2007), Ziffer 1.6.1.

461 So auch Huhn/Pfitzmann, Technische Randbedingungen jeder Kryptoregulierung, verfügbar unter: http://events.ccc.de/congress/1995/div/pfitz/krypto.htm (18.12.2006): „So müssen Sicherheitsparameter wie die Schlüssellänge danach eingestellt werden, ob es dem Benutzer wichtiger ist, in kurzer Zeit große Datenmengen zu verarbeiten, deren Vertraulichkeit oder Integrität nur über Wochen garantiert werden muß, oder ob die Daten über Jahrzehnte geschützt werden sollen, so daß auch Angriffe mit erheblich gesteigerter Rechenleistung berücksichtigt werden müssen.“

462 Vergleiche zum staatlichen Gewaltmonopol *Nitz*, Private und öffentliche Sicherheit, S. 313 ff.

den Staat (zumindest auch) wegen des Selbsthilfeverbots und als Kompensation dafür[463] gewährleistet; greift der Einzelne aber zur Selbsthilfe, mag das staatliche Sanktionen auslösen, es beraubt ihn aber nicht staatlichen Schutzes. Schließlich zeigt das anerkannte Prinzip der Notwehr bzw. Nothilfe, dass der Staat Selbstschutz durchaus billigt – freilich zumeist nur dann, wenn effektiver staatlicher Schutz nicht oder nicht rechtzeitig erreichbar ist.

Welche konkreten Schutzmaßnahmen den gewährten staatlichen Schutz in diesem Sinne hinreichend effektiv machen mag zwar grundsätzlich einem weiten Einschätzungsspielraum unterliegen,[464] Grenze ist aber das Untermaßverbot.[465] Kommunikationsdaten werden nicht nur durch Private, die der inländischen Jurisdiktion unterliegen, abgehört, sondern sind vor allem auch erstens durch Abhörmaßnahmen *aus dem Ausland* und zweitens durch Abhörmaßnahmen ausländischer *staatlicher* Akteure gefährdet:[466]

> "Internet transactions and email between Europeans is increasingly sent through servers in the US. In many ways this situation is similar to the SWIFT case: transactions between two individuals in Europe may well transit through US telecommunications companies and as a result will be made accessible to the US government. This activity involves no oversight or legal protections for non-U.S. persons. As a result, the communications of European citizens are completely vulnerable to abuse."[467]

Kann der Staat Taten von Privatpersonen im Ausland immerhin noch dem deutschen Strafrecht unterstellen bei einem hinreichenden Inlandsbezug (vgl. etwa die

463 *Robbers*, Sicherheit als Menschenrecht, S. 127.

464 Siehe in Teil 6 unter A.I.4.b.

465 Vergleiche Teil 6 unter A.I.4.c.

466 Vergleiche dazu etwa ein jüngst in Schwedens verabschiedetes Gesetz, das dem dortigen militärischen Abschirmdienst („Försvarets radioanstalt" – FRA) gestattet, die gesamte elektronische Kommunikation mit dem Ausland via Internet oder Telefon zu überwachen; heise online vom 18.06.2008, Widerstand gegen umfassendes Abhörgesetz in Schweden, verfügbar unter: http://www.heise.de/newsticker/Widerstand-gegen-umfassendes-Abhoergesetz-in-Schweden--/meldung/109644 (25.06.2008). Dadurch wird aber auch deutscher E-Mail-Verkehr u.U. abgehört, wenn er über schwedische Server geroutet wird. Die für das Routing von Datenpaketen zuständigen Protokolle orientieren sich nicht an Landesgrenzen; heise online vom 24.03.2009, Nationale Filterregeln und die globalen Datenströme, verfügbar unter: http://www.heise.de/newsticker/Nationale-Filterregeln-und-die-globalen-Datenstroeme--/meldung/135042 (25.03.2009). Derartiges könnte zwar implementiert werden, verursacht bei den Providern aber Kosten; vgl. Scheuring, The Pirate Bay rüstet auf, verfügbar unter: http://www.heise.de/tp/r4/artikel/28/28190/1.html (03.07.2009). Ob sich teurere, aber vor verdachtslosem Abhören sichere Kommunikation als privates Geschäftsmodell am Markt positionieren kann ohne staatlichen Druck, erscheint fraglich. In Serbien soll lt. heise online vom 03.08.2008, Serbische Polizei will E-Mails überwachen, verfügbar unter: http://www.heise.de/newsticker/Serbische-Polizei-will-E-Mails-ueberwachen--/meldung/113731 (05.08.2008) Polizei und Geheimdienst uneingeschränkter Zugriff auf elektronische Post bei serbischen Internet Providern gewährt werden.

467 American Civil Liberties Union (ACLU) in einem Schreiben an den Vorsitzenden der Artikel-29-Datenschutzgruppe, zitiert nach Statewatch, The Shape of Things to Come, verfügbar unter: http://www.statewatch.org/analyses/the-shape-of-things-to-come.pdf (11.09.2008), S. 12.

Ausdehnung deutscher Strafgewalt nach §§ 5-7 StGB[468]) und auf diesem Weg Schutzmaßnahmen treffen (wie effektiv diese auch sein mögen), so ist ihm dieses Vorgehen gegenüber ausländischen (Sicherheits)Behörden wegen des völkerrechtlichen Grundsatzes der staatlichen Immunität verwehrt. Fremde Hoheitsakte („acta iure imperii“) unterliegen nach diesem Grundsatz nicht der staatlichen Jurisdiktion eines anderen Staates.[469] Einseitig kann der Staat hier folglich keinen effektiven rechtlichen Schutz gewähren.[470] Ein Verbot technischer Selbstschutzmaßnahmen würde den Einzelnen diesen Gefahren gegenüber schutzlos lassen.[471]

(g) Parallelwertung zum Briefgeheimnis

Schließlich ist für das Briefgeheimnis unzweifelhaft, dass mittels Briefumschlags gegen Kenntnisnahme geschützte Sendungen vom Schutzbereich umfasst sind.[472] Maßnahmen zum Schutz gegen Kenntnisnahme sind im Rahmen des Fernmeldegeheimnisses parallel zu werten:

> „Wie die erwähnte Diskussion um den Schutzbereich des Briefgeheimnisses zeigt, ist die Frage der Existenz und Nutzung von Selbstschutzmöglichkeiten nicht ohne Belang für die Frage der Anwendbarkeit des Art. 10 GG. Dann wäre es jedoch mit dem Zweck des Art. 10 unvereinbar, solche Selbstschutzmöglichkeiten im Bereich der modernen Telekommunikation aus dem grundrechtlichen Schutzbereich von vornherein auszuklammern. Als ein – möglicherweise sogar unentbehrliches – Hilfsmittel, die Vertraulichkeit der Kommunikation unter den besonderen technischen Gegebenheiten des Internet sicherzustellen, wird der Gebrauch solcher

468 Eine weitere Ausdehnung der staatlichen Strafgewalt findet sich in dem in § 1 VStGB niedergelegten Weltrechtsprinzip zur Verfolgung von Verbrechen gegen die Menschlichkeit. Hierbei ist zwar nach dem Wortlaut der Norm noch nicht mal ein Inlandsbezug erforderlich, de facto wird ein solcher gerade wegen des Immunitätsgrundsatzes aber doch verlangt, vgl. § 153f StPO sowie Der Generalbundesanwalt beim Bundesgerichtshof, Pressemitteilung vom 10.02.2005, verfügbar unter: http://www.generalbundesanwalt.de/prnt/showpress.php?newsid=163 (25.06.2008).

469 *Epping*, in: *Ipsen,* Völkerrecht, § 26, Rn. 18.

470 Bi- oder multilaterale Vereinbarungen wären möglich, internationale Einigkeit auf diesem Gebiet herzustellen scheint unwahrscheinlich angesichts der betroffenen vitalen staatlichen Eigeninteressen.

471 Soweit *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 120 ff. betont, dass sich aus von auswärtiger öffentlicher Gewalt drohenden Grundrechtsgefahren *keine* staatlichen Schutzpflichten ergeben, steht diese Aussage dem nicht entgegen. Vielmehr basieren die Ausführungen *Isensees* gerade auf der erläuterten Unmöglichkeit effektiven rechtlichen Schutzes gegenüber ausländischen Hoheitsträgern. Es gibt insoweit keinen *rechtlichen* Schutz und der Staat schuldet auch keinen solchen. Ein Verbot technischer Selbstschutzmaßnahmen würde in einer derartigen Situation aber einen eigenen staatlichen Eingriff in das Fernmeldegeheimnis in seiner abwehrrechtlichen Dimension bedeuten. Letztlich kommt es darauf aber nicht an, da Gefahren sowohl von inländischen wie von ausländischen Angreifern herrühren.

472 *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 27; *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 31; *Löwer*, in: *v. Münch/Kunig,* GG, Art. 10, Rn. 16; teilweise wird die Verschlossenheit sogar als Voraussetzung für die Eröffnung des Schutzbereichs angesehen, vgl. *Groß,* JZ 1999, 326, 332. Auch das LG Köln vergleicht in seinem Urteil vom 28.05.2008, Az.: 28 O 157/08, Rn. 29 (juris) eine E-Mail mit einem verschlossenen Brief.

Verschlüsselungstechniken vielmehr vom Schutzbereich des Fernmeldegeheimnisses ebenso mitumfaßt wie die Versendung von Briefumschlägen bei der Briefpost vom Schutz des Briefgeheimnisses."[473]

(h) Ergebnis

Daher muss auch die Übermittlung verschlüsselter Daten vom Schutzbereich des Fernmeldegeheimnisses umfasst sein.

cc) Postgeheimnis

Neben der Eröffnung des Schutzbereichs des Fernmeldegeheimnisses ist kein Raum für eine Eröffnung des Schutzbereichs des Postgeheimnisses. Anknüpfungspunkt des Postgeheimnisses war traditionell die Inanspruchnahme eines bestimmten Kommunikationsmittlers, der staatlichen Postverwaltung.[474] Das gilt weiterhin, auch wenn Nachfolgeunternehmen der Deutschen Bundespost als Telekommunikationsmittler in Anspruch genommen werden. Mit der Auflösung (oder dem Wegfall) der Deutschen Bundespost und dem Funktionsübergang auf Privatunternehmen sind Bedeutung und Inhalt des Postgeheimnisses zwar zunehmend fraglich geworden.[475] Es herrscht jedoch weitgehend Einigkeit darüber, dass jedenfalls das Fernmeldegeheimnis einen Spezialfall des Postgeheimnisses darstellt, der die gesamte nichtkörperliche Individualkommunikation umfasst.[476] Die voranschreitende Auflösung des staatlich monopolisierten Postwesens spricht für diese Orientierung am Übermittlungsmedium und den Abschied von der überkommenen Fixierung auf die Deutsche Bundespost als Übermittler. Der Schutzbereich des Postgeheimnisses ist daher, soweit es wie hier um nicht-körperliche Daten geht, nicht eröffnet.[477]

473 *Grote,* KritV 1999, 27, 40 f.

474 *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 44; *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 32.

475 Inwieweit können die Nachfolgeunternehmen überhaupt noch als „Post" angesehen werden? Wer ist grundrechtsberechtigt und wer grundrechtsverpflichtet aus dem Postgeheimnis? Für einen Wegfall des Gegenstandes des „Postgeheimnisses" plädiert etwa *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 46.

476 BVerfGE 67, 157, 172 – strategische Überwachung; *Jarass/Pieroth,* GG, Art. 10, Rn. 4; *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 33; *Löwer*, in: *v. Münch/Kunig,* GG, Art. 10, Rn. 17; *Hadamek*, Art. 10 GG und die Privatisierung der Deutschen Bundespost, S. 212; a.A. nur *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 63.

477 *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 33.

b. Verschlüsselungsverfahren im Schutzbereich des Art. 10 I GG

Zu prüfen ist, ob der Schutzbereich des Fernmeldegeheimnisses neben der Übermittlung verschlüsselter Daten auch die Generierung verschlüsselter Daten, also den Verschlüsselungsvorgang selbst, umfasst.

aa) Verschlüsselung als rechtlich unabhängiger Vorgang?

Gegen eine Eröffnung des Schutzbereichs auch für den Verschlüsselungsvorgang könnte sprechen, dass die der Datenübermittlung lediglich zeitlich vor- bzw. nachgelagerte Ver- bzw. Entschlüsselung als rechtlich unabhängiger Vorgang einzuordnen sein könnte.[478] Zutreffend ist sicher, dass die bloße *Intention* einer späteren Übermittlung nicht für die Eröffnung des Schutzbereichs von Art. 10 I GG ausreichend sein kann.[479] Wenn jemand Daten im Hinblick auf eine spätere Übermittlung verschlüsselt, diese Daten aber zunächst für unbestimmte Zeit auf seinem Rechner speichert, liegt offensichtlich (noch) kein Anwendungsfall des Fernmeldegeheimnisses vor.[480] Werden aber Daten vom Versender für die Übermittlung verschlüsselt und im Anschluss daran tatsächlich versandt, ist die Annahme einer echten Zäsur zwischen den Vorgängen Verschlüsselung einerseits und Übermittlung andererseits Fiktion, und zwar sowohl bei rein tatsächlicher[481] als auch daran anknüpfend bei rechtlicher Betrachtungsweise. Der offenkundige, finale Zusammenhang kann bei einer rechtlichen Bewertung nicht gänzlich außer Betracht bleiben.

Die Betrachtung des Einsatzes von Verschlüsselungsverfahren bei Anonymisierungsdiensten zur Gewährleistung der Vertraulichkeit von Kommunikationsumständen bestätigt dies: Verschlüsselungs- und Übermittlungsvorgang sind ein technisch und zeitlich untrennbarer Vorgang.

bb) Verschlüsselung als Grundrechtsverwirklichung

Der Einsatz von Verschlüsselungsverfahren dient damit unmittelbar der Verwirklichung des grundrechtlich durch das Fernmeldegeheimnis gewährleisteten Schutzes,

478 So etwa *Meyn*, Verschlüsselung und Innere Sicherheit, S. 55 ff., der die Frage als Gesichtspunkt der zeitlichen Dimension des Fernmeldegeheimnisses versteht.

479 Vergleiche die Ausführungen und das Bespiel bei *Meyn*, Verschlüsselung und Innere Sicherheit, S. 57.

480 Im Fall der parallelen Fragestellung nach dem zeitlichen Ende des Schutzes des Fernmeldegeheimnisses hat das Bundesverfassungsgericht dieses nicht mehr für einschlägig gehalten, wenn sich die Daten „im Herrschaftsbereich des Empfängers, der eigene Schutzvorkehrungen gegen den ungewollten Datenzugriff treffen kann," befinden; BVerfG, Urteil vom 02.03. 2006, Az.: 2 BvR 2099/04, Rn. 73.

481 Vergleiche etwa die Figur der natürlichen Handlungseinheit im Strafrecht.

nämlich der Vertraulichkeit räumlich distanzierter Kommunikation. Darüber hinaus wird in der Literatur teilweise vertreten, Art. 10 I GG gewährleiste auch die Verfügungsbefugnis über kommunikationsbezogene Informationen.[482] Diese Verfügungsbefugnis wird danach etwa durch den Einsatz von Verschlüsselungsverfahren verwirklicht.[483] Da Art.10 I GG Teil des grundgesetzlichen Privatsphärenschutzes ist, gewährleiste dieser in Parallele zum allgemeinen Persönlichkeitsrecht und zum Recht auf informationelle Selbstbestimmung auch einen Schutz der Selbstbestimmung über Informationen.[484] Daher sei auch die Entscheidung, Kommunikation durch technische Selbstschutzmaßnahmen zu schützen, vom Fernmeldegeheimnis umfasst:

> „Das BVerfG präzisiert den Schutz des Kommunikationsinhalts auch im Hinblick auf die Subjekte des Grundrechtsschutzes. Danach ist es „Sache der am Kommunikationsvorgang Beteiligten, darüber zu bestimmen, wer von dem Inhalt Kenntnis erlangen soll". Es ist daher nicht nur der Inhalt der Nachricht grundrechtsgeschützt, sondern auch die Entscheidungs- und Verfügungsbefugnis der Beteiligten, ihr Geheimnis selbst zu schützen. Aus diesem Grund ist der Geheimnisschutz nicht auf das Haben des Geheimnisses beschränkt, sondern beinhaltet auch die Freiheit, es selbst mit technischen Mitteln zu schützen."[485]

c. Zusammenfassung

Der Schutzbereich des Art. 10 I GG ist für alle Arten von Daten eröffnet, sowohl verschlüsselte als auch unverschlüsselte. Das Fernmeldegeheimnis schützt umfassend die Übermittlung von Daten im Wege der Fernmeldetechnik. Der Schutz des Fernmeldegeheimnisses erfasst darüber hinaus die Verwendung von Verschlüsselungsverfahren, um die Vertraulichkeit von Daten bei der fernmeldetechnischen Übermittlung zu gewährleisten. Das Fernmeldegeheimnis schützt also sowohl die vertrauliche Kommunikation selbst als auch deren anonyme Übermittlung.

482 *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 15; *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 186; *Bizer,* KritJ 1995, 450, 454. In eine ähnliche Richtung weist die Rechtsprechung des BVerfG, die betont, dass sich die Schutzwirkung des Art. 10 I GG nicht nur auf den ersten Zugriff der öffentlichen Gewalt auf Telekommunikationsvorgänge und –inhalte bezieht, sondern „sich auch auf die Informations- und Datenverarbeitungsprozesse [erstreckt], die sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließen, und auf den Gebrauch, der von den erlangten Kenntnissen gemacht wird."; BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 190.

483 So etwa *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 186.

484 *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 15 f.; *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 186; a.A. dagegen *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 81 ff.

485 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 186.

2. Grundrechtseingriff durch ein absolutes Verschlüsselungsverbot

Ein absolutes Verbot von Verschlüsselungsverfahren würde einen Eingriff in das Fernmeldegeheimnis aus Art. 10 I GG bedeuten, der verfassungsrechtlich gerechtfertigt werden müsste.

> "Eine gegenüber den Nutzern von Informations- und Kommunikationstechnik greifende Untersagung, ihre Kommunikation selbst zu schützen, oder eine Einschränkung ihres Selbstschutzes durch die Beschränkung auf zugelassene Verfahren stellt einen Eingriff in Art. 10 Abs. 1 GG dar."[486]

> „Ein Verbot von Anonymisierungsdiensten für E-Mail mit dem Zweck, die anonyme Kommunikation über E-Mail zu verhindern, wäre genau darauf angelegt, das Fernmeldegeheimnis der Nutzer mittelbar zu beschränken, und folglich ein Eingriff in ihre durch Art. 10 Abs. 1 GG geschützten Rechte.“[487]

3. Verfassungsrechtliche Rechtfertigung eines absoluten Verschlüsselungsverbots

a. Gesetzesvorbehalt

Einschränkungen des Art. 10 I GG sind nur auf Grund eines Gesetzes möglich, Art. 10 II S. 1 GG. Ein derartiges formelles oder materielles Gesetz existiert derzeit für die Bundesrepublik Deutschland nicht. Die Verwendung von Verschlüsselungsverfahren ist daher bisher uneingeschränkt erlaubt. Auf die Möglichkeit eines Wiederauflebens der Forderungen nach einem Verbot von Verschlüsselungsverfahren wurde bereits hingewiesen. Es ist ungewiss, inwieweit strafprozessuale oder sicherheitsbehördliche Ermittlungsmaßnahmen bisher durch den Einsatz von Verschlüsselungsverfahren be- oder gänzlich verhindert wurden. Klar ist aber, dass eine zukünftige massenhafte Nutzung von Verschlüsselungstechnologien die Debatte um einen adäquaten Umgang mit dieser Technologie neu entfachen würde, und es daher nicht als ausgeschlossen angesehen werden kann, dass ein entsprechendes Gesetz erlassen würde.

b. Verstoß gegen die Wesensgehaltsgarantie (Art. 19 II GG)

Ein solches absolutes Verschlüsselungsverbotsgesetz könnte in den durch Art. 19 II GG geschützten grundrechtlichen Wesensgehalt von Art. 10 I GG eingreifen, da ein effektives Mittel zum Schutz der Vertraulichkeit der privaten Fernkommunikation untersagt würde.

486 *Marauhn,* KritV 1999, 57, 80.
487 *Möller,* DuD 2000, 267, 270.

aa) Bedeutung der Wesensgehaltsgarantie

Fraglich ist, ob der Schranken-Schranke des Art. 19 II GG neben dem Verhältnismäßigkeitsgrundsatz noch eigenständige Bedeutung zukommt. Wurde vom BVerfG zunächst noch häufig auf die Wesensgehaltsgarantie Bezug genommen,[488] ist heute ein Funktionsverlust des Art. 19 II GG zu konstatieren,[489] der sicher auch dem Erstarken des allgemeinen Verhältnismäßigkeitsgrundsatzes zum zentralen Instrument der materiellen Sicherung der Grundrechte geschuldet ist.[490] Möchte man nicht an eine verfassungsgeberische Redundanz glauben, ist aber von einer eigenständigen Bedeutung der Wesensgehaltsgarantie auszugehen.[491] Diese Sichtweise scheint auch in der Rechtsprechung des BVerfG anzuklingen:

> „Der schwerwiegende Grundrechtseingriff […] verstößt nicht gegen die Wesensgehaltsgarantie, solange gewichtige Schutzinteressen Dritter den Eingriff zu legitimieren vermögen und insbesondere der Grundsatz der Verhältnismäßigkeit gewahrt ist.“[492]

bb) Bestimmung des Wesensgehalts

In der Literatur ist umstritten, worin der Wesensgehalt eines Grundrechts besteht und wie dieser bestimmt werden kann. Weitgehende Einigkeit herrscht zumindest insoweit, dass der Wesensgehalt für jedes Grundrecht gesondert zu bestimmen ist:

> „Der unantastbare Wesensgehalt eines Grundrechts muss für jedes Grundrecht aus seiner besonderen Bedeutung im Gesamtsystem der Grundrechte ermittelt werden.“[493]

(1) Qualität des Wesensgehalts

Während die einen[494] davon ausgehen, dass jedes Grundrecht über einen absolut geschützten Kernbereich als Wesensgehalt verfügt (absolute Theorie), begreift die Gegenauffassung[495] den Wesensgehalt als abwägungsfähige, variable Größe (relative Theorie). Die Rechtsprechung des BVerfG erlaubt keine eindeutige Positionsbestimmung,[496] zumal die Wesensgehaltsgarantie in der verfassungsgerichtlichen

488 *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 110 mit Rechtsprechungsnachweisen.
489 So *Dreier*, in: *Dreier,* GG, Art. 19 II, Rn. 8.
490 *Dreier*, in: *Dreier,* GG, Art. 19 II, Rn. 8; *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 110 ff.; *Sachs*, in: *Sachs,* GG, Art. 19, Rn. 40.
491 So auch *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 175 ff.; *Heß*, Grundrechtskonkurrenzen, S. 116.
492 BVerfG, Urteil vom 05.02.2004, Az.: 2 BvR 2029/01, Rn. 96.
493 BVerfG, Urteil vom 05.02.2004, Az.: 2 BvR 2029/01, Rn. 96.
494 *Jarass/Pieroth,* GG, Art. 19, Rn. 9; *Sachs*, in: *Sachs,* GG, Art. 19, Rn. 43 f.; weitere Nachweise bei *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 139 ff.
495 *Dreier*, in: *Dreier,* GG, Art. 19 II, Rn. 16; weitere Nachweise bei *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 142 ff.
496 Wie *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 149 ff. herausgearbeitet hat.

Rechtsprechung weitgehend bedeutungslos geworden ist.[497] Es wurde bereits überzeugend nachgewiesen, dass sich absolute und relative Theorie, die in ihrer jeweiligen „Reinform" gar nicht mehr vertreten zu werden scheinen,[498] in ihren neueren Ausprägungen in der Literatur in einem Annäherungsprozess befinden: Die absolute Theorie tendiert dazu, den absolut geschützten Kernbereich vor allem in den objektiv-institutionellen Grundrechtsgehalten zu sehen.[499] Die relative Theorie zeigt dagegen Tendenzen, einen „abwägungsresistenten" Bereich zu betonen, in dem mit hoher Wahrscheinlichkeit kein das Eingriffsrechtsgut überwiegender Rechtfertigungsgrund existieren kann.[500]

(2) Gewährleistungsgehalt des Art. 19 II GG

Umstritten ist daneben auch, ob zur Bestimmung des Wesensgehalts auf die Grundrechtsbestimmung als objektive Norm abzustellen ist (institutionelle Ausrichtung), oder ob die subjektive Rechtsposition des individuellen Grundrechtsträgers ebenfalls in den Blick zu nehmen ist (personalistische Ausrichtung).[501] Dies hängt zwar sicherlich mit der ebenfalls diskutierten Frage, ob die Wesensgehaltsgarantie neben dem objektiv-rechtlichen Schutz auch ein subjektives Recht vermittelt,[502] zusammen, ist aber von dieser zu trennen.[503]

Bei Zugrundelegung einer institutionellen Betrachtungsweise dient Art. 19 II GG der Gewährleistung des Wesensgehalts des Grundrechts *als solchem*. Dem ist Genüge getan, wenn einer hinreichend großen Zahl an Grundrechtsträgern ein hinreichend großer Teil der grundrechtlich geschützten Rechtspositionen verbleibt. Bei Zugrundelegung einer personalistischen Betrachtungsweise gewährleistet die Wesensgehaltsgarantie *dem Einzelnen* wirkungsvollen Grundrechtsschutz. Dieser Ansicht ist zu folgen. Nach der Grundkonzeption und dem ursprünglichen Sinn der Grundrechte sind diese subjektive Abwehrrechte des Einzelnen gegen den Staat.[504] Grundrechte gewähren gerade dem Einzelnen individuelle Rechte.[505]

497 *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 110.
498 *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 147.
499 *Dreier*, in: *Dreier,* GG, Art. 19 II, Rn. 12.
500 *Alexy*, Theorie der Grundrechte, S. 271 f.
501 Vgl. zum Streitstand m.v.w.N. *Dreier*, in: *Dreier,* GG, Art. 19 II, Rn. 12 ff.
502 Bejahend *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 174; *Krebs*, in: *v. Münch/Kunig,* GG, Art. 19, Rn. 24.
503 Literatur wie BVerfG scheinen insoweit zur Annahme eines subjektiv-rechtlichen Charakters zu neigen, vgl. *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 174. Der Fragestellung kommt im Rahmen dieser Arbeit untergeordnete Bedeutung zu, da die (objektive) Verfassungsmäßigkeit von Verschlüsselungsrestriktionen untersucht werden soll und nicht die (wenngleich praktisch äußerst bedeutsame) Möglichkeit der gerichtlichen Geltendmachung subjektiver Betroffenheit.
504 *Dreier*, in: *Dreier,* GG, Vorbemerkung, Rn. 84.
505 Davon wiederum sorgfältig zu trennen ist die Frage nach der gerichtlichen Durchsetzbarkeit des subjektiven Rechts.

„Es hieße deshalb „ … den ursprünglichen und bleibenden Sinn der Grundrechte gerade dort zu verkehren, wo es um … ihr Wesen geht", wollte man den Individualbezug an dieser Stelle ausblenden. Es ist m. a. W. gerade das „Wesen" eines Grundrechts (im Sinne des Grundgesetzes), dass es *sich im konkreten Fall* bewährt."[506]

Daher muss der *Einzelne jeweils wirkungsvollen Grundrechtsschutz* genießen.[507]

Problematisch sind insoweit allerdings die Fälle der restlosen Entziehung einer Grundrechtsposition im Einzelfall: der so genannte „finale Rettungsschuss" vernichtet das durch Art. 2 II S. 1 GG geschützte Leben; die lebenslange Freiheitsstrafe entzieht das in Art. 2 II S. 2 GG geschützte Recht auf Freiheit der Person. Beides verstößt – Rechtsprechung und Literatur zufolge – nicht gegen die Wesensgehaltsgarantie des Art. 19 II GG.[508] Beide Fälle scheinen sich auf den ersten Blick nur mit einem institutionellen Ansatz vereinbaren zu lassen. Art. 2 II S. 3 GG zeigt aber bereits, dass nach dem Grundgesetz selbst das Leben nicht vorbehaltlos gewährleistet ist.[509] Teilweise wird in der Literatur zwischen Grundrecht und Schutzgut differenziert.[510] Zum Wesen eines Grundrechts gehört demnach neben der Existenz eines Schutzgutes vor allem ein wirksamer Schutzmechanismus. Hinsichtlich des Schutzgutes reicht es danach aus, wenn ein hinreichend großes Segment der geschützten Interessen verbleibt, das Schutzgut also nicht zum „nudum ius" wird.[511] Die entscheidende Gewährleistung der Wesensgehaltsgarantie ist danach die effektive Kontrolle sämtlicher Eingriffe:

„Dabei kommt es nicht darauf an, ob der einzelne Grundrechtsträger „nach dem Eingriff noch in der Lage ist, das betreffende Grundrecht in Bezug auf von ihm zu bestimmende Rechtsobjekte in ausreichenden Maße zu aktualisieren", sondern nur darauf, ob er in der Lage ist, sich gegen staatliche Beeinträchtigungen des durch das Grundrecht effektiv geschützten Lebensbereichs wirkungsvoll zur Wehr zu setzen."[512]

Zu in der Sache ähnlichen Ergebnissen gelangt auch eine andere Literaturmeinung, die eine personalistische Betrachtungsweise mit der relativen Theorie kombiniert.[513] Lückenlos überzeugen kann wohl keiner der derzeit vertretenen Ansätze zur Bestimmung des Wesensgehalts, woraus sicherlich auch das Kaleidoskop der verschiedenen Theorien resultiert. Im Ergebnis kann jedenfalls festgehalten werden, dass auch der vollständige Entzug einer Rechtsposition im Einzelfall keine Verlet-

506 *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 170 unter Zitierung von *Herbert*, EuGRZ 1985, 321, 324.

507 So auch *Dreier*, in: *Dreier,* GG, Art. 19 II, Rn. 12; *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 169 ff..

508 Zur lebenslangen Freiheitsstrafe vgl. BVerfGE 45, 187, 270 f.; zum finalen Rettungsschuss vgl. *Schulze-Fielitz*, in: *Dreier,* GG, Art. 2 II, Rn. 118; *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 1, Rn. 78 m.w.N.

509 *Dreier*, in: *Dreier,* GG, Art. 19 II, Rn. 13.

510 *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 153 ff.

511 *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 156.

512 *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 162 unter Zitierung von *Denninger*, in: AK GG, Art. 19 Abs. 2, Rn. 6 f.

513 *Dreier*, in: *Dreier,* GG, Art. 19 II, Rn. 16.

zung der Wesensgehaltsgarantie darstellen muss, solange grundsätzlich der Schutz des Rechtsguts gewährleistet ist.

> „Der Wesensgehalt eines Grundrechts ist das substantielle Minimum, bei dessen Verletzung der verbleibende Rest, auch wenn er den Namen des vollen Rechts weiterführt, nicht mehr in wesensmäßiger Identität mit diesem steht. Diese Identitätsschwelle kann sowohl durch qualitative Eingriffe als auch durch starke quantitative Rechtsminderungen überschritten werden; es gibt auch hier einen Umschlag aus der Quantität in die Qualität."[514]

Die Wesensgehaltsgarantie dient somit der

> „Sicherung der Grundrechtssubstanz vor einem unbeschränkten, ohne eine derartige Sicherungszone zur vollständigen Entleerung und praktischen Auslöschung des Grundrechts führenden Zugriffs des einfachen Gesetzgebers."[515]

(3) Verhältnis von Wesensgehalt zu Menschenwürdegehalt

Noch nicht vollständig geklärt ist auch das Verhältnis der Wesensgehaltsgarantie zum spezialgrundrechtlichen Menschenwürdegehalt. Beide sind jedenfalls nicht vollkommen identisch:[516] Art. 19 II GG wäre überflüssig, wenn der Wesensgehalt vollständig im grundrechtlichen Menschenwürdegehalt aufginge.[517] Systematisch ebenfalls nicht erklärbar wäre auch, weshalb die Ewigkeitsgarantie des Art. 79 III GG auf die Menschenwürde, nicht aber auf die Wesensgehaltsgarantie nach Art. 19 II GG Bezug nimmt.[518]

Daraus kann schon abgeleitet werden, dass der Wesensgehalt eines Grundrechts nach der verfassungsrechtlichen Konzeption *mehr* umfassen muss als den durch die Ewigkeitsgarantie absolut gesicherten Kernbestand.[519] Art. 19 II GG schützt folglich mehr als den grundrechtlichen Menschenwürdegehalt, zumindest aber diesen. Daher folgt aus einer Verletzung des Menschenwürdegehalts eines Grundrechts stets auch eine Verletzung seines Wesensgehalts.[520]

514 *Huber,* DÖV 1956, 135, 142.
515 *Dreier*, in: *Dreier,* GG, Art. 19 II, Rn. 7.
516 Diese These wurde lt. *Dreier*, in: *Dreier,* GG, Art. 1, Rn. 163 sowie *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 1, Rn. 34, jeweils m.w.N. vor allem von *Dürig* aufgestellt, gilt heute aber als widerlegt.
517 *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 126; *Sachs*, in: *Sachs,* GG, Art. 19, Rn. 43.
518 Zu den Argumenten im Einzelnen vgl. *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 125 ff.
519 So auch *Sachs*, in: *Sachs,* GG, Art. 19, Rn. 44; *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 130, 132.
520 So auch *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn.127 ff. mit vielen weiteren Nachweisen.

cc) Antastung des Wesensgehalts des Fernmeldegeheimnisses durch ein absolutes Verschlüsselungsverbot

Zu prüfen ist, ob danach ein absolutes Verschlüsselungsverbotsgesetz den Wesensgehalt des Fernmeldegeheimnisses antastet.

(1) Widerspruch zur Ideengeschichte des Fernmeldegeheimnisses

Für eine Antastung des Wesensgehalts spricht, dass ein Verbot von Selbstschutzmaßnahmen mit der Finalität der Aufrechterhaltung staatlicher Kenntnisnahmemöglichkeiten einen Bruch mit der Ideengeschichte des Fernmeldegeheimnisses bedeuten würde.[521] Art. 10 GG verfügt über zwei Schutzrichtungen, einerseits gegenüber der Kenntnisnahme Dritter – vor allem der Postbediensteten – und andererseits gerade auch gegenüber der Kenntnisnahme durch staatliche Sicherheitsbehörden:

> „Seine besondere Bedeutung gewinnt es aus der Erfahrung, dass der Staat unter Berufung auf seine eigene Sicherheit sowie die Sicherheit seiner Bürger häufig zum Mittel der Überwachung privater Kommunikation gegriffen hat. Dabei kommt ihm zustatten, dass als Vermittler überwiegend die staatlich betriebene Post auftritt. Der Zugriff wird dadurch sowohl leichter als auch unauffälliger. Die Tragweite des Postgeheimnisses ist daher verkürzt, wenn man es primär als Schutz vor den Bediensteten der Post ansieht. Der Grundrechtsschutz bezieht sich historisch und aktuell vor allem auf die staatlichen Sicherheitsbehörden. Dementsprechend hat das Bundesverfassungsgericht herausgestellt, dass Art. 10 GG nicht nur den Einzelnen gegenüber der Post, sondern auch Bürger und Post gegenüber anderen staatlichen Stellen schützt.“[522]

Auch wenn die besondere Situation der staatlichen Übermittlertätigkeit heute so nicht mehr fortbesteht, hat dies an der Grundkonzeption der zwei Schutzrichtungen nichts geändert. Zumal im Rahmen der Privatisierung der Post von staatlicher Seite durchaus darauf geachtet worden ist, sich die erleichterten Zugriffsmöglichkeiten zu erhalten.[523] Ein Verbot effektiver Schutzmöglichkeiten zu Gunsten der Erhaltung staatlicher Abhöroptionen bedeutet daher eine grundlegende Abwendung von der Kernidee, die das Brief-, Post- und Fernmeldegeheimnis inhaltlich ausmachen.

(2) Umkehrung verfassungsrechtlicher Grundsatzwertungen

Für eine Antastung des grundrechtlichen Wesensgehalts spricht weiter, dass ein absolutes Verschlüsselungsverbotsgesetz eine Umkehrung der grundrechtsimmanenten Systematik impliziert. Das Grundgesetz geht nach seiner Konstruktion zunächst vom Zustand der Freiheit aus. Der Zustand, der herrscht, soweit keine anderen Regelungen getroffen wurden, ist grundsätzlich der der Freiheit des Individuums,[524] so wie

521 So auch *Marauhn,* KritV 1999, 57, 81.
522 BVerfGE 85, 386, 396.
523 *Marauhn,* KritV 1999, 57, 69.
524 So auch *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 22.

sie durch die speziellen und allgemeinen Freiheitsgrundrechte zum Ausdruck kommt. Demgegenüber ist der Eingriff in diese Freiheitsrechte rechtfertigungsbedürftig.[525] Dieser Grundsatz würde durch ein Verschlüsselungsverbot genau in sein Gegenteil verkehrt:

> „Ein präventives Verbot derartiger individueller Schutzmaßnahmen würde die Wahrnehmung der Verschlüsselungsoption von vornherein als `verdächtig´ diskreditieren und unter einen grundsätzlichen Ausübungsvorbehalt stellen. Damit wäre nicht mehr der staatliche Eingriff in das Fernmeldegeheimnis rechtfertigungsbedürftig, sondern der individuelle Schutz des Fernmeldegeheimnisses mit Hilfe von Verschlüsselungsmaßnahmen.“[526]

(3) Erhalt traditioneller Schutzmöglichkeiten

Gegen eine Antastung des Wesensgehalts könnte sprechen, dass durch ein Verbot der Verwendung von Verschlüsselungsverfahren der grundrechtliche Schutz an sich nicht beeinträchtigt wird. Die fernmeldetechnisch übermittelte Kommunikation wird nach wie vor durch das Fernmeldegeheimnis vor der unbefugten Kenntnisnahme Dritter geschützt. Der allein durch ein rechtliches Kenntnisnahmeverbot gesicherte Schutz mag geringer sein als der technisch vermittelte Schutz von Verschlüsselungsverfahren, gleichwohl handelt es sich um grundrechtlichen Schutz. Der Schutz des Fernmeldegeheimnisses an sich steht rechtlich nicht zur Disposition. Faktisch mag das Fernmeldegeheimnis heute durch Internationalisierung und Digitalisierung anderen Gefährdungen ausgesetzt sein, auf die der Staat angemessen reagieren müsste, um den grundrechtlichen Schutz weiterhin zu gewährleisten. Es handelt sich dabei aber um eine Frage der Qualität des Schutzes, während die Wesensgehaltsgarantie zunächst auf die prinzipielle Anerkennung des Schutzgutes gerichtet ist.

(4) Unzureichender tatsächlicher Schutz

Andererseits kann die bloße prinzipielle Anerkennung eines Schutzgutes nicht ausreichend sein, wenn zugleich der faktische Grundrechtsschutz nahezu vollständig ausgehöhlt ist. Dies ist – wie *Huber* formuliert hat – der Fall, wenn

> „[..] der verbleibende Rest [eines Grundrechts; d. Verf.], auch wenn er den Namen des vollen Rechts weiterführt, nicht mehr in wesensmäßiger Identität mit diesem steht. Diese Identitätsschwelle kann sowohl durch qualitative Eingriffe als auch durch starke quantitative Rechtsminderungen überschritten werden; es gibt auch hier einen Umschlag aus der Quantität in die Qualität.“[527]

Daraus folgt, dass zumindest eine gewisse Effektivität des tatsächlichen Grundrechtsschutzes gewährleistet sein muss – in qualitativer wie quantitativer Hinsicht:

525 *Kutscha*, Innere Sicherheit und Freiheitsrechte, in: *Roggan/Kutscha,* Handbuch zum Recht der Inneren Sicherheit, S. 28, 29.
526 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 204.
527 *Huber,* DÖV 1956, 135, 142.

Wenn in der digitalen Welt niemand mehr vertraulich kommunizieren kann, da jede Kommunikation von jedem beliebigen Interessierten mitgelesen und alle Kommunikationsumstände überwacht werden können (*quantitative Perspektive*), dann ist dies wesensmäßig kein Fernmelde*geheimnis* mehr. Genau dies wäre die Situation bei Erlass eines absoluten Verschlüsselungsverbotsgesetzes. Der grundrechtliche Schutz wäre bei einem Verbot des technischen Schutzes durch Verschlüsselungsverfahren – in Anlehnung an die Umschreibung von *Dreier*[528] - „vollständig entleert und praktisch ausgelöscht". Andere w*irksame*, insbesondere rechtliche Schutzmechanismen sind angesichts der Transnationalität des Internets und den damit einhergehenden Rechtsverfolgungs- und Rechtsdurchsetzungsdefiziten nicht ersichtlich.

(5) Unantastbarer Kernbereich privater Lebensgestaltung

In einer *qualitativen Perspektive* würde durch ein absolutes Verschlüsselungsverbotsgesetz auch der Schutz von Kommunikation, die zum unantastbaren Kernbereich privater Lebensgestaltung gehört, untersagt.

Nach der Rechtsprechung des BVerfG gewährleistet die Menschenwürde (Art. 1 I GG) einen unantastbaren Kernbereich privater Lebensgestaltung:

> „Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen. Vom Schutz umfasst sind auch Gefühlsäußerungen, Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität."[529]

Dieser Kernbereichsschutz gehört zum Menschenwürdegehalt des Fernmeldegeheimnisses (Art. 10 I GG). Antastungen dieses Kernbereichs stellen sich nach der Rechtsprechung des BVerfG[530] nicht als unmittelbare Verletzungen des Art. 1 I GG, sondern als Verletzung des Fernmeldegeheimnisses dar:

> „Art. 10 Abs. 1 GG gewährleistet die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Kommunikation und schützt damit zugleich die Würde des Menschen. Die nach Art. 1 Abs. 1 GG stets garantierte Unantastbarkeit der Menschenwürde fordert auch im Gewährleistungsbereich des Art. 10 Abs. 1 GG Vorkehrungen zum Schutz individueller Entfaltung im Kernbereich privater Lebensgestaltung."[531]

Eine eigenständige Prüfung einer Verletzung der Menschenwürde (Art. 1 I GG) kommt daneben nicht mehr in Betracht.[532] Eine Verletzung des Menschenwürdege-

528 *Dreier*, in: *Dreier,* GG, Art. 19 II, Rn. 7, vergleiche oben.
529 BVerfG, Urteil vom 03.03.2004, Az.: 1 BvR 2378/98 und 1 BvR 1084/99, Rn. 120.
530 Vgl. *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 1, Rn. 28 m.w.N.; *Dreier*, in: *Dreier,* GG, Art. 1, Rn. 162.
531 BVerfG, Urteil vom 27.07.2005, Az.: 1 BvR 668/04, Rn. 162 f.
532 Unabhängig von der Frage, ob Art. 1 I GG eigene Grundrechtsqualität aufweist (so *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 1, Rn. 28) oder in einem „Fundierungsverhältnis" zu den Spezialgrundrechten steht (so *Dreier*, in: *Dreier,* GG, Art. 1, Rn. 162).

halts des Fernmeldegeheimnisses bedeutet dabei zugleich eine Antastung des Wesensgehalts von Art. 10 I GG – so zumindest für den Schutz eines unantastbaren Kernbereichs privater Lebensgestaltung auch das BVerfG:

> „Das Bundesverfassungsgericht erkennt jedoch einen letzten unantastbaren Bereich privater Lebensgestaltung an, der der öffentlichen Gewalt schlechthin entzogen ist. Selbst schwerwiegende Interessen der Allgemeinheit können Eingriffe in diesen Bereich nicht rechtfertigen; eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes findet nicht statt. Dies folgt einerseits aus der Garantie des Wesensgehalts der Grundrechte (Art. 19 Abs. 2 GG), zum anderen leitet es sich daraus ab, daß der Kern der Persönlichkeit durch die unantastbare Würde des Menschen geschützt wird."[533]

Soweit mit dem unantastbaren Kernbereich privater Lebensgestaltung der Menschenwürdegehalt eines Spezialgrundrechts betroffen ist, unterfällt dieser ebenso der Ewigkeitsgarantie des Art. 79 III GG wie Art. 1 I GG selbst – jedenfalls nach der Rechtsprechung des BVerfG zum Kernbereichsschutz im Rahmen des „großen Lauschangriffs".[534]

> „Zwar wird es stets Formen von besonders gravierender Kriminalität und entsprechende Verdachtssituationen geben, die die Effektivität der Strafrechtspflege als Gemeinwohlinteresse manchem gewichtiger erscheinen lässt als die Wahrung der menschlichen Würde des Beschuldigten. Eine solche Wertung ist dem Staat jedoch durch Art. 1 Abs. 1, Art. 79 Abs. 3 GG verwehrt."[535]

Ist der unantastbare Kernbereich privater Lebensgestaltung betroffen, liegt folglich eine nicht zu rechtfertigende Verletzung des jeweiligen Spezialgrundrechts, hier des Fernmeldegeheimnisses, vor. Ein solcher durch die Ewigkeitsgarantie (Art. 79 III GG) auch gegen Verfassungsänderungen gesicherter Gewährleistungskern muss Teil des grundrechtlichen Wesensgehalts nach Art. 19 II GG sein – jedes andere Verständnis wäre zutiefst widersprüchlich.

Regelmäßig können Maßnahmen, die unter Umständen diesen Kernbereich privater Lebensgestaltung berühren können (siehe etwa die Rechtsprechung des BVerfG zur akustischen Wohnraumüberwachung[536] oder zur präventiven Telekommunikationsüberwachung[537]), nach der Rechtsprechung des BVerfG durch verfahrensmäßige Vorkehrungen gegen Kernbereichseingriffe sowie nachträgliche Verwertungsverbote und Löschungspflichten so ausgestaltet werden, dass kein Verstoß gegen den grundrechtlichen Menschenwürde- und Wesensgehalt (mehr) vorliegt.

Die Besonderheit eines absoluten Verschlüsselungsverbots ist, dass solche prozeduralen Ausgestaltungen in der digitalen Welt keinen als äquivalent anzusehenden Kernbereichsschutz gewährleisten können. Dies mag zwar gegenüber staatlichen Eingriffen (siehe das Beispiel Telekommunikationsüberwachung) noch möglich sein, das Fernmeldegeheimnis schützt aber auch vor den aus der Übermittlung resultierenden Gefahren der Kenntnisnahme Dritter, insbesondere der Übermittler.

533 BVerfGE 80, 367, 373 f. – Tagebuchaufzeichnungen.
534 A.A. *Dreier*, in: *Dreier,* GG, Art. 79 III, Rn. 28 m.w.N.
535 BVerfG, Urteil vom 03.03.2004, Az.: 1 BvR 2378/98 und 1 BvR 1084/99, Rn. 121.
536 BVerfG, Urteil vom 03.03.2004, Az.: 1 BvR 2378/98 und 1 BvR 1084/99.
537 BVerfG, Urteil vom 27.07.2005, Az.: 1 BvR 668/04.

Übermittler kann bei internetbasierter Kommunikation aber jeder sein – er muss nur einen Router betreiben (dies können ausländische Unternehmen sein, beliebige Privatpersonen etc.). Rechtliche prozedurale Maßnahmen können insbesondere gegenüber ausländischen Kommunikationsmittlern nicht wirksam durchgesetzt werden.

Besteht für Informationen, die zum absolut geschützten Kernbereich privater Lebensgestaltung gehören, im Rahmen von Kommunikation weder ein wirksamer prozeduraler Schutz noch die Möglichkeit technischen Schutzes gegen Kenntnisnahme , dann tastet dies den Wesensgehalt des Fernmeldegeheimnisses an (*qualitative Perspektive*). Ein absolutes Verschlüsselungsverbotsgesetz würde den Kernbereich privater Lebensgestaltung und damit den Menschenwürdegehalt von Art. 10 I GG berühren und gegen die Wesensgehaltsgarantie verstoßen.

dd) Ergebnis

Ein absolutes Verschlüsselungsverbotsgesetz würde daher nach hier vertretener Auffassung gegen die Wesensgehaltsgarantie (Art. 19 II GG) verstoßen. Angesichts der Zurückhaltung von BVerfG wie Literatur, einen Verstoß gegen die Wesensgehaltsgarantie anzunehmen, und der festgestellten Verlagerung der zugrundliegenden Fragestellungen auf die Verhältnismäßigkeitsebene wird hier, obwohl mit der Annahme eines Verstoßes gegen die Wesensgehaltsgarantie die Verfassungswidrigkeit eines absoluten Verschlüsselungsverbotsgesetzes nach hier vertretener Auffassung bereits feststeht, dennoch auch die Verhältnismäßigkeit geprüft.

c. Verhältnismäßigkeitsgrundsatz

Ein Gesetz, das ein absolutes Verbot von Verschlüsselungsverfahren vorsieht, könnte auch gegen den Verhältnismäßigkeitsgrundsatz verstoßen. Eine einfachgesetzliche Norm, die ein solches Verbot festschreiben würde, müsste einem legitimen Zweck dienen, zur Erreichung dieses Zwecks geeignet und erforderlich sein sowie in einer Gesamtabwägung verhältnismäßig im engeren Sinne sein.

aa) Legitimer Zweck

Ein absolutes Verschlüsselungsverbotsgesetz müsste zunächst einem legitimen Zweck zu dienen bestimmt sein. Im Hinblick auf die Einschätzungsprärogative des Gesetzgebers scheiden an dieser Stelle nur Zwecke aus, die bereits an sich klar verfassungswidrig sind.[538] Der Prüfungspunkt dient daher eher der Benennung und

538 So auch *Meyn*, Verschlüsselung und Innere Sicherheit, S. 103; *Jakobs*, Der Grundsatz der Verhältnismäßigkeit, S. 60 verortet diese Frage bei der Prüfung der Geeignetheit.

Konkretisierung der verfolgten Zwecke als ihrer Prüfung und Bewertung.[539] Anhand dieser Zielsetzung beurteilen sich schließlich Geeignetheit und Erforderlichkeit.

Ein absolutes Verschlüsselungsverbot soll verhindern, dass die sicherheitsbehördlichen Ermittlungsinstrumente, die auf das Abhören oder die sonstige Kenntnisnahme von Daten gerichtet sind, de facto sinnlos werden.[540] Der dahinter stehende Zweck ist zweifelsohne legitim: Straftaten sollen, soweit möglich, verhindert, in jedem Falle aber effektiv verfolgt werden. Angesichts international vernetzt operierender Strukturen aus dem Bereich der organisierten Kriminalität und der latenten Bedrohung durch den internationalen Terrorismus[541] erscheint ein Arsenal (höchst) effektiver Ermittlungsmethoden zu Gunsten der Sicherheitsbehörden dringend geboten. Unabhängig von der Frage nach der Existenz eines „Grundrechts auf Sicherheit“[542] stellen Verbrechensbekämpfung und wirksame Strafverfolgung Gemeinwohlbelange von hohem verfassungsrechtlichen Rang dar, wie das BVerfG immer wieder hervorgehoben hat:

> „Der Verhinderung und Aufklärung von Straftaten kommt nach dem Grundgesetz hohe Bedeutung zu. Das BVerfG hat deshalb wiederholt die unabweisbaren Bedürfnisse einer wirksamen Strafverfolgung und Verbrechensbekämpfung hervorgehoben, das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren – zur Überführung von Straftätern ebenso wie zur Entlastung Unschuldiger – betont und die wirksame Aufklärung gerade schwerer Straftaten als einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet.“[543]

Daneben kommt dem Gemeinwohlinteresse an der Sicherung des Rechtsfriedens, dem Verfolgung und Verhütung von Straftaten dienen, nach der Rechtsprechung des BVerfG zusätzliches eigenständiges Gewicht zu.[544]

> „Die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit sind Verfassungswerte, die mit anderen hochwertigen Gütern im gleichen Rang stehen. Die Schutzpflicht findet ihren Grund sowohl in Art. 2 Abs. 2 Satz 1 als auch in Art. 1 Abs. 1 Satz 2 GG. Der Staat kommt seinen verfassungsrechtlichen Aufgaben nach, indem er Gefahren durch terroristische oder andere Bestrebungen entgegen tritt. Die vermehrte Nutzung elektronischer oder digitaler Kommunikationsmittel und deren Vordringen in nahezu alle Lebensbereiche erschwert es der Verfassungsschutzbehörde, ihre Aufgaben wirkungsvoll wahrzunehmen. Auch extremistischen und terroristischen Bestrebungen bietet die moderne Informationstechnik zahlreiche Möglichkeiten zur Anbahnung und Pflege von Kontakten sowie zur Planung und Vorbereitung, aber auch Durchführung von Straftaten. Maßnahmen des Gesetzgebers, die informationstechnische Mittel für staatliche Ermittlungen erschließen, sind insbesondere vor dem Hin-

539 Zu den Fragen der Argumentationslast, des Nachschiebens von Zwecken sowie der Austauschbarkeit von Mittel und Zweck vergleiche ausführlich *Schlink*, Abwägung im Verfassungsrecht, S. 203 ff sowie *Meyn*, Verschlüsselung und Innere Sicherheit, S. 99 ff.

540 *Meyn*, Verschlüsselung und Innere Sicherheit, S. 102.

541 Zwei Bedrohungsszenarien, die zugegebenermaßen zur Begründung vielfältiger Sicherheitsgesetze bereits arg strapaziert worden sind.

542 Vgl. insoweit vor allem *Isensee*, Das Grundrecht auf Sicherheit; *Robbers*, Sicherheit als Menschenrecht.

543 BVerfG, Urteil vom 14.07.1999, Az.: 1 BvR 2226/94 et al., Rn. 260.

544 BVerfG, Urteil vom 27.07.2005, Az.: 1 BvR 668/04, Rn. 148.

tergrund der Verlagerung herkömmlicher Kommunikationsformen hin zum elektronischen Nachrichtenverkehr und der Möglichkeiten zur Verschlüsselung oder Verschleierung von Dateien zu sehen."[545]

Die genannten Zwecke Strafverfolgung, Verbrechensprävention und Sicherung des Rechtsfriedens stellen gewichtige Allgemeinwohlbelange dar und sind folglich legitim.

bb) Geeignetheit

Ein solches Gesetz zum absoluten Verbot von Verschlüsselungsverfahren müsste zur Erreichung der angestrebten Zwecke geeignet sein. Dies ist der Fall, „wenn mit seiner Hilfe der gewünschte Erfolg gefördert werden kann."[546] An einer solchen Förderung des verfolgten Zweckes könnte es hier aber fehlen, da ein absolutes Verschlüsselungsverbot ein praktisch äußerst ineffektives Instrument zur Aufrechterhaltung von Überwachungsoptionen staatlicher Sicherheitsbehörden ist (Ziffern (1) bis (5)). Zu erörtern bleibt, wann eine Maßnahme einen solchen Grad an Ineffektivität erreicht hat, dass man nicht mehr von einer Förderung des gewünschten Erfolges und damit von Geeignetheit sprechen kann. Die Umgehungsmöglichkeiten berauben ein absolutes Verschlüsselungsverbotsgesetz aber nicht jeglicher Legitimation und Wirkung (Ziffern (6) und (7)). Für die Bejahung der Geeignetheit spricht schließlich der dem Gesetzgeber vom BVerfG zugebilligte weite Einschätzungsspielraum (vergleiche Ziffer (9)) ebenso wie die Erkenntnis, dass optimales staatliches Handeln häufig unmöglich sein wird (siehe unter Ziffer (8)).

(1) Einfache Umgehungsmöglichkeiten

Gegen die Geeignetheit eines absoluten Verschlüsselungsverbotsgesetzes zur Sicherung staatlicher Kenntnisnahmeoptionen spricht, dass ein solches Verbot ohne Weiteres umgangen werden kann. Starke Verschlüsselungsverfahren sind überall auf der Welt via Internet unproblematisch erhältlich.[547] Ihre Handhabung erfordert keine besonderen Kenntnisse oder Fähigkeiten.[548] Letztlich bedarf es noch nicht einmal des Rückgriffs auf ein bereits bestehendes Verschlüsselungsverfahren. Jeder kann mit einem Einmalschlüssel-Verfahren (`*One-Time-Pad´*) Daten mit einem beliebigen Codewort oder Schlüssel verschlüsseln.[549] Eine solche Einmalverschlüsselung ist

545 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 220.
546 BVerfGE 30, 292, 316 sowie jüngst BVerfG, Beschluss vom 24.09.2009, Az.: 1 BvR 1231/04 et al., Rn. 5.
547 *Bizer*, Verschlüsselung und staatlicher Datenzugriff, in: *Büllesbach,* Datenschutz im Telekommunikationsrecht, S. 245, 263; *Koch,* CR 1997, 106, 108; *Roßnagel,* ZRP 1997, 26, 27; *Trute,* JZ 1998, 822, 829.
548 *Koch,* CR 1997, 106, 107; *Trute,* JZ 1998, 822, 829.
549 Siehe dazu oben in Teil 1 unter A.I.3.

zwar für den Massengebrauch in der Praxis wenig praktikabel, für Kriminelle, Terroristen etc. aber durchaus attraktiv: Es ist nicht nur absolut sicher, sondern auch so einfach, dass es schon mit geringen Informatikkenntnissen programmiert werden kann.[550] Mit einer Anleitung aus dem Internet dürfte nahezu jeder dazu in der Lage sein.

(2) Schwierige Feststellbarkeit der Umgehung des Verbots

Gegen die Geeignetheit eines absoluten Verschlüsselungsverbots spricht weiter, dass ohne Kenntnis des verwendeten Verschlüsselungsverfahrens nicht ohne Weiteres festgestellt werden kann, dass Daten überhaupt verschlüsselt wurden. Soweit die Daten dem Schutzbereich des Fernmeldegeheimnisses unterfallen, ist eine staatliche Kenntnisnahme nur zur Verfolgung und Verhütung schwerer Straftaten verfassungsgemäß.[551] Ein Verstoß gegen das Verschlüsselungsverbot könnte also nur festgestellt werden, wenn der Betreffende oder einer seiner Kommunikationspartner aus anderen Gründen in den Fokus der Sicherheitsbehörden geraten würde. Den Daten selbst ist ohne inhaltliche Kenntnisnahme nicht anzusehen, ob sie verschlüsselt sind oder nicht.

(3) Problematische Etablierung von Kontrollbefugnissen

Gegen die Geeignetheit spricht auch, dass die Schaffung neuer Kontrollbefugnisse zur Überwachung der Einhaltung des Verschlüsselungsverbots verfassungsrechtlich problematisch wäre. Ein Gesetz, das derartige Kontrollbefugnisse schaffen würde, wäre ebenfalls am Fernmeldegeheimnis zu messen. Effektive Kontrolle wäre dabei nur zu erreichen, wenn diese verdachtsunabhängig oder unter geringen Voraussetzungen erfolgen könnte. Dies wäre aber mit dem Fernmeldegeheimnis nicht in Einklang zu bringen.[552] Bei hohen Voraussetzungen ergäbe sich eine parallele Eingriffsschwelle wie sie jetzt für Überwachungsmaßnahmen besteht. Die Etablierung weitergehender Kontrollbefugnisse zur Überwachung der Einhaltung eines Verschlüsselungsverbots ist nicht in verfassungsgemäßer Weise möglich.[553]

550 Laut *Koch,* CR 1997, 106, 107 wär ein Schüler nach einem halben Jahr Informatikunterricht dazu in der Lage.

551 Vgl. insoweit BVerfG, Urteil vom 27.07.2005, Az.: 1 BvR 668/04, Rn. 152 ff.

552 So auch *Rihaczek*, Kryptokontroverse und Normung, in: *Tinnefeld/Köhler/Piazolo,* Arbeit in der mobilen Kommunikationsgesellschaft, S. 270, 272.

553 Soweit eingewandt wurde, die Verwendung verbotener Verschlüsselungsverfahren könne zum Anlass für weiterführenden Ermittlungen genommen werden (vgl. Schulzki-Haddouti, TP: Kanthers Kurs auf das Kryptoverbot, verfügbar unter: http://www.heise.de/tp/r4/artikel/1/1146/2.html (01.12.2008)), ist dies verfassungsrechtlich ebenfalls bedenklich, da Verschlüsselung auch dem Schutz legitimer Privatheitsinteressen dient. Ob sich aus der Wahrung legitimer, grundrechtlich geschützter Interessen Verdachtsmomente zur Rechtfertigung (weiter-

(4) „Verstecken“ der verschlüsselten Daten

Gegen eine Geeignetheit eines absoluten Verschlüsselungsverbotsgesetzes spricht ferner, dass verschlüsselte Daten mittels Steganographie effektiv versteckt werden können. Sicherheitsbehörden können dann noch nicht einmal herausfinden, dass überhaupt (weitere) Daten vorhanden sind.[554] Dies könnte nur durch ein Verbot des Versands von Bild- und Musikdateien, die derzeit meist zum Verstecken von Nachrichten verwendet werden, verhindert werden.[555] Auch dies würde einen Eingriff in das Fernmeldegeheimnis bedeuten, der verfassungsrechtlich nicht zu rechtfertigen wäre, da nur im Wege der inhaltlichen Kenntnisnahme „erlaubte“ von „verbotenen“ Daten unterschieden werden könnten.

(5) Unmöglichkeit wirksamer Sanktionierung eines Verstoßes gegen das Verschlüsselungsverbot

Zweifel an der Geeignetheit eines absoluten Verschlüsselungsverbotsgesetzes ergeben sich ferner aus der Unmöglichkeit einer angemessenen Sanktionierung von Verstößen gegen das Verbot. Da die Daten nicht entschlüsselt werden können, kann bei der Sanktionierung von Verstößen gerade nicht an den Inhalt der verschlüsselten Daten angeknüpft werden. Eine Differenzierung zwischen Datenverschlüsselung zu strafbaren Zwecken und solchen zu legitimen Zwecken ist nicht möglich.[556] Sollte man angesichts des legitimen Interesses des Privatsphärenschutzes überhaupt eine Strafandrohung für verhältnismäßig halten,[557] müsste diese jedenfalls sehr gering ausfallen.[558] Bei geringer Strafhöhe verliert eine solche Androhung aber weitgehend ihren Sinn, da sie gerade im Zusammenhang mit schwerwiegenden Straftaten für die

gehender) sicherheitsbehördlicher Ermittlungstätigkeit ergeben können, erscheint äußerst fraglich.

554 *Dix,* CR 1997, 38, 42; *Federrath*, Steganographie – vertrauliche Kommunikation ohne Kryptographie, in: *Hamm/Möller,* Datenschutz durch Kryptographie, S. 42, 47; *Weichert,* DuD 2007, 590, 591; so auch bereits BVerfG, Urteil vom 14.07.1999, Az.: 1 BvR 2226/94 et al., Rn. 216.

555 *Koch,* CR 1997, 106, 109.

556 Dies wird beispielsweise in Frankreich und anderen Staaten (eine Übersicht s.o. in Teil 2 unter B.III.) anders gesehen: Nach Art. 132-79 Code pénal erhöht sich jeweils der Strafrahmen, wenn zur Begehung oder Vorbereitung der Straftat Verschlüsselungsverfahren eingesetzt wurden. Es zeigt sich aber auch, dass die Regelung nicht für Ordnungswidrigkeiten und Straftaten, die mit einer Höchststrafe unter drei Jahren bedroht sind, gilt. Dem könnten ähnliche Überlegungen zur Verhältnismäßigkeit zu Grunde liegen, wie sie hier angestellt werden. Über die Strafandrohung soll aber vor allem die Herausgabe von Schlüsseln und Passwörtern erzwungen werden. Ausführlich dazu unten in Teil 5.

557 Insoweit ebenfalls zweifelnd *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 207.

558 *Koch,* CR 1997, 106, 109.

Täter nicht ins Gewicht fällt.[559] Schließlich ist der Beweis, dass Daten verschlüsselt wurden, unter Umständen[560] schwierig zu erbringen. Wenn nicht die Entschlüsselung gelingt, könnte es sich bei den Daten auch um ein Computerprogramm, eine komprimierte Datei[561] oder schlicht um Datenschrott handeln.[562]

(6) Kein grundsätzliches Legitimationsdefizit auf Grund von Umgehungsmaßnahmen

Für die Geeignetheit eines absoluten Verschlüsselungsverbotsgesetzes spricht dagegen, dass eine Norm nicht schon dadurch ihren Sinn und ihre Legitimation verliert, dass sie umgangen werden kann oder umgangen wird.[563] Bei Zugrundelegung eines solchen Maßstabs wären viele Gesetze als ungeeignet und damit als verfassungswidrig anzusehen. So wird beispielsweise niemand ernstlich die Sinnhaftigkeit und Legitimität des strafrechtlichen Tötungsverbotes bezweifeln – obwohl die Existenz der angestrebten generalpräventiven Abschreckungswirkung umstritten ist.[564] Fehlte es an einer Abschreckungswirkung des Tötungsverbots, würde das eigentliche Schutzgut Leben durch die Strafandrohung überhaupt nicht (effektiv) geschützt. Der Täter wird nur im Nachhinein bestraft. Der Wert eines strafrechtlichen Verbots dürfte da-

559 Die Bundesregierung vertritt dagegen in ihrer Antwort auf eine Kleine Anfrage (BT-Drs. 13/1676) die Ansicht, dass eine Sanktionierung von Verstößen gegen ein Verschlüsselungsverbot zum einen möglich wäre und zum anderen Abschreckungswirkung entfalten würde; BT-Drs. 13/1889, S. 3.

560 In den Fällen, in denen der Header entfernt wurde; *Koch,* CR 1997, 106, 109.

561 Nach *Heuser*, Verschlüsselung im Spannungsfeld von staatlichem Anspruch und individueller Freiheit, in: *Kubicek,* Multimedia – Technik sucht Anwendung, S. 224, 227 sind die Grenzen zwischen Datenkompression und Verschlüsselung ohnehin fließend.

562 *Koch,* CR 1997, 106, 109 weist zusätzlich darauf hin, dass bei der Verwendung von Remailern verschlüsselte Daten auch anonym versandt werden können, so dass noch nicht einmal der Täter zu ermitteln wäre.

563 *Koch,* CR 1997, 106, 109. Grenze ist eine reine Symbolgesetzgebung (dazu unten im Rahmen der Prüfung eines möglichen Gleichheitsverstoßes (C.) mehr): „Dass sich u.U. Einzelne illegal verhalten, spricht nicht gegen die Geeignetheit einer Maßnahme. Anderes muss jedoch dann gelten, wenn von vornherein nicht davon ausgegangen werden kann, dass ein Verbot in erwähnenswertem Umfang Beachtung findet"; *Manssen*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 12, Rn. 135.

564 So auch *Meyn*, Verschlüsselung und Innere Sicherheit, S. 116. Vergleiche auch *Streng*, Strafrechtliche Sanktionen, Rn. 59: „Die Abschreckungsidee hat nur für begrenzte Deliktsbereiche im Bagatellbereich, wo die Regelbefolgung relativ wenig gewissensgestützt ist, und zudem nur in recht schwacher Form empirische Abstützung erhalten". *Streng* weist aber zuvor unter Rn. 56 auch darauf hin, dass die empirischen Befragungen unter den gesellschaftlichen Bedingungen der Existenz eines strafrechtlichen Systems entstanden und somit von dieser Prämisse nicht zu trennen seien. Siehe zum derzeitigen Forschungsstand zur generalpräventiven Wirkung strafrechtlicher Sanktionen Bundesministerium des Innern/Bundesministerium der Justiz, Zweiter Periodischer Sicherheitsbericht, verfügbar unter: http://www.bmj.bund.de/files/-/1485/2.%20Periodischer%20Sicherheitsbericht%20Langfassung.pdf (15.01.2008), S. 685 f. sowie *Meier*, Strafrechtliche Sanktionen, S. 27 ff.

her unter anderem auch in der (gesellschaftlichen) Ächtung eines Verhaltens zu sehen sein.[565] Auch darin liegt ein legitimer politischer und gesetzgeberischer Wille.[566]

(7) Keine umfassende Missachtung eines Verschlüsselungsverbots

Für die Geeignetheit eines absoluten Verschlüsselungsverbots spricht weiter, dass ein strafbewehrtes Verbot durchaus eine Hürde darstellt, die ein auf seine Außenwirkung bedachtes Unternehmen oder einen *`white-collar´*-Kriminellen von seiner Missachtung abhalten würde.[567] Immerhin würde die Grenze der Legalität klar überschritten. Dies erfordert zumindest ein gewisses Maß an krimineller Energie. Auch erfordert der Einsatz von Verschlüsselungsverfahren einen gewissen Aufwand, den viele nicht bereit sind zu treiben.[568] Eine vollständige Missachtung und Umgehung eines Verschlüsselungsverbots wäre jedenfalls kaum zu erwarten. Damit kann einem Verbot auch nicht jede Eignung abgesprochen werden.

565 Dies deckt sich mit den Erkenntnissen der neueren kriminologischen Forschung: „Die erwartete Schwere der Strafe für bestimmte Taten erwies sich als bedeutungslos. Das wahrgenommene Entdeckungsrisiko zeigte sich nur bei einer Reihe leichterer Delikte als immerhin etwas relevant. Als wesentlich wichtigerer Erklärungsfaktor für Normkonformität trat die wahrgenommene moralische Verbindlichkeit der Strafnorm bzw. die Strafnormakzeptanz in Erscheinung.“, *Streng*, Strafrechtliche Sanktionen, S. Rn. 55; so auch *Meier*, Strafrechtliche Sanktionen, S. 28.

566 Grenze des gesetzgeberischen Einschätzungsspielraums könnte insoweit rein symbolische Gesetzgebung sein. Dies wird unten unter C. noch näher zu erörtern sein.

567 So *Heuser*, Verschlüsselung im Spannungsfeld von staatlichem Anspruch und individueller Freiheit, in: *Kubicek,* Multimedia – Technik sucht Anwendung, S. 224, 227.

568 Der Anteil verschlüsselter Daten am Datenverkehr via Internet liegt lt. heise online vom 18.12.2008, Internet-Anwender sind Verschlüsselungsmuffel, verfügbar unter: http://www.heise.de/newsticker/Internet-Anwender-sind-Verschluesselungsmuffel--/meldung/120671 (19. 12.2008) zwischen fünf und 15 Prozent – ohne Verschlüsselungsverbot. Laut heise online vom 06.07.2008, Umfrage: Fast 4 Millionen deutsche Opfer von Computer-Kriminalität, verfügbar unter: http://www.heise.de/newsticker/Umfrage-Fast-4-Millionen-deutsche-Opfer-von-Computer-Kriminalitaet--/meldung/110494 (07.07.2008) haben sogar 28 Prozent der Computernutzer ein Verschlüsselungsprogramm auf ihrem privaten Rechner installiert. Die Diskrepanz dieser Angaben könnte im befragten Personenkreis sowie darin begründet liegen, dass die Verschlüsselungsprogramme selten oder jedenfalls nicht für alle Datenübermittlungen eingesetzt werden. Zudem erzeugen manche Anwendungen signifikant mehr Datenverkehr als andere: So erzeugt etwa das Herunterladen von Musik oder Filmen, was regelmäßig nicht verschlüsselt erfolgen dürfte, ein hohes Maß an Datenverkehr, während eine E-Mail, zu deren Verschlüsselung Nutzer vielleicht eher neigen, nur wenig Datenverkehr generiert. Schließlich könnten – angesichts des Wissens um die Kenntnisnahmeoptionen bei Datenübermittlungen im Internet – auch Nutzer den Einsatz von Verschlüsselungsprogrammen behauptet haben, die ein solches praktisch kaum einsetzen.

(8) Unmöglichkeit optimalen staatlichen Handelns

Für die Geeignetheit eines Verschlüsselungsverbots spricht auch, dass in vielen Konstellationen optimaler staatlicher Schutz objektiv nicht erreichbar ist. Würde man vom Staat nur optimale Schutzmaßnahmen akzeptieren, würde dies bei Unerreichbarkeit optimalen Schutzes (was wohl der Regelfall sein dürfte) bedeuten, auch auf die staatlichen Schutzmaßnahmen zu verzichten, die möglich wären. Damit würde dem Einzelnen nicht nur kein optimaler, sondern im Ergebnis überhaupt kein Schutz seiner Interessen gewährt. Dies kann nicht Sinn und Zweck der Forderung nach möglichst effektivem Schutz sein.

(9) Weiter Einschätzungsspielraum des Gesetzgebers

Für die Geeignetheit eines absoluten Verschlüsselungsverbots spricht zuletzt der weite Einschätzungsspielraum, den das BVerfG dem Gesetzgeber zubilligt.[569] Diesen Einschätzungsspielraum sieht das BVerfG nur dann als überschritten an, wenn eine Maßnahme überhaupt nichts zur Förderung des verfolgten Zweckes beitragen kann oder sogar kontraproduktiv wirkt:[570]

> „Auf Gesetzesebene genügt es, wenn die abstrakte Möglichkeit der Zweckerreichung besteht, die zugelassenen Maßnahmen also nicht von vornherein untauglich sind, sondern dem gewünschten Erfolg förderlich sein können."[571]

Die Entscheidung hingegen, welcher Förderungsgrad wie schwerwiegende Eingriffe in andere Rechtsgüter zu legitimieren vermag, verlagert das BVerfG in die im Rahmen der Verhältnismäßigkeit im engeren Sinne stattfindende Gesamtabwägung.[572]

(10) Ergebnis

Da man einem absoluten Verschlüsselungsverbotsgesetz nicht von vornherein jedwede Wirkung absprechen kann, ist bei Zugrundelegung der Rechtsprechung des BVerfG ein solches Verbot (noch) als geeignet anzusehen.[573] Mit dem BVerfG ist dem Gesetzgeber insoweit ein weiter Einschätzungs- und Prognosespielraum zuzubilligen, der hier nicht überschritten wird. Die im Rahmen der Verhältnismäßigkeit

569 Vergleiche dazu ausführlich *Meyn*, Verschlüsselung und Innere Sicherheit, S. 104 ff.
570 *Jakobs*, Der Grundsatz der Verhältnismäßigkeit, S. 59 f. m.w.N.
571 BVerfG, Urteil vom 14.07.1999, Az.: 1 BvR 2226/94 et al., Rn. 214.
572 Eine nennenswerte Begrenzungs- oder Filterfunktion kann so in der Prüfung der Geeignetheit nur schwerlich gesehen werden.
573 Eine ähnliche Diskussion wird hinsichtlich der Geeignetheit von Internetsperren zum Schutz vor rechtsextremistischen oder kinderpornographischen Inhalten geführt. Vgl. dazu *Höhne/ Dienst,* juris PR ITR 13/2009 sowie ausführlich *Sieber/Nolde*, Sperrverfügungen im Internet, S. 180 ff., insbes. 193 ff., die zu ähnlichen Ergebnissen wie hier kommen.

im engeren Sinne durchzuführende Gesamtabwägung wird allerdings das dargestellte bedeutende Umgehungspotential berücksichtigen müssen.

cc) Erforderlichkeit

Ein absolutes Verschlüsselungsverbotsgesetz müsste zur Erreichung der angestrebten Zwecke auch erforderlich sein. Eine Maßnahme ist erforderlich,

> „wenn der Gesetzgeber nicht ein anderes, gleich wirksames, aber das Grundrecht nicht oder doch weniger fühlbar einschränkendes Mittel hätte wählen können."[574]

Teilweise wurde in der Literatur die Auffassung vertreten, ein Verschlüsselungsverbot sei nicht erforderlich, da die Sicherheitsbehörden auf andere Weise[575] – etwa durch V-Leute oder die Infiltration von Rechnern (Online-Durchsuchung) – an die Schlüssel gelangen könnten. Eine Entschlüsselung verschlüsselter Daten sei daher möglich, ein Verschlüsselungsverbot nicht erforderlich. Offensichtlich ist, dass Durchsuchung und Beschlagnahme nach §§ 102, 103, 94 StPO jedenfalls keine Alternativen sind, da es sich im Gegensatz zu Maßnahmen der Überwachung von E-Mail, Internetzugang und Telekommunikation um lediglich punktuelle Maßnahmen handelt, die zudem offen stattfinden.[576] Die insbesondere für Strukturermittlungen notwendige längerfristige heimliche Überwachung kann so nicht ersetzt werden. Als tauglich könnten sich dagegen der Einsatz verdeckter Ermittler nach § 110a StPO sowie sonstige Observationsmaßnahmen nach § 100f StPO oder Maßnahmen der akustischen Wohnraumüberwachung nach § 100c StPO erweisen. Inwieweit diese Maßnahmen tatsächlich Überwachungsmaßnahmen bezüglich E-Mail, Telekommunikation oder Internetzugang ersetzen könnten und ob dies im Hinblick auf die durch die genannten Maßnahmen bedingten Grundrechtseingriffe (etwa in Art. 13 Abs. 1 GG) vorzugswürdig ist, kann allerdings nur schwer bewertet werden:[577]

574 BVerfGE 30, 292, 316.

575 *Koch,* CR 1997, 106, 109; *Marauhn,* KritV 1999, 57, 79 nannten vor allem den Einsatz von V-Leuten, Computerviren oder Seitenkanalangriffe (Seitenkanalangriffe versuchen, aus äußerlich physikalisch messbaren Größen wie Rechenzeit, Stromverbrauch oder elektromagnetischer Abstrahlung Rückschlüsse auf ausgeführte Rechenoperationen und damit letztlich auf den verwendeten Schlüssel zu erlangen; vgl. Wikipedia, Seitenkanalattacke, Version vom 02.07.2009, 14.51 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Seitenkanalattacke&oldid=61795510) als Alternativen. Heute ist zudem an die im Rahmen der Online-Durchsuchung diskutierten Infiltrationstechniken zu denken, die sich aber im Kern nicht vom Szenario „Computerviren" unterscheiden dürften.

576 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 206.

577 *Andrzejak*, Kryptoregulierung, in: *Hoeren/Queck,* Rechtsfragen der Informationsgesellschaft, S. 132, 141 f. verweist auf eine US-amerikanische Studie, derzufolge die Verwendung von Verschlüsselungsverfahren die Strafverfolgung und Beweisfindung nicht gehindert habe, da entweder der Schlüssel erlangt werden, die Verschlüsselung gebrochen oder anderweitige Beweise gefunden werden konnten. Die Studie weist aber auch darauf hin, dass sich dies mit weiterer Verbreitung der Nutzung von Verschlüsselungsverfahren ändern könnte.

Die genannten Vorgehensweisen dienen zwar auch dem Zweck der Aufrechterhaltung sicherheitsbehördlicher Kenntnisnahmeoptionen. Es ist aber zweifelhaft, ob diese Verfahren *genauso* geeignet sind wie ein Verschlüsselungsverbot: Der Gesetzgeber kann nur insoweit auf ein milderes Mittel verwiesen werden, als dieses zur Zweckerreichung in *gleicher* Weise geeignet ist. Die hier vorgeschlagenen Alternativen stoßen – wie ein absolutes Verschlüsselungsverbot (s.o. unter bb)) – ebenfalls auf Schwierigkeiten und an technische Grenzen, allerdings auf andere Schwierigkeiten und Grenzen. Je nach Konstellation im Einzelfall kann die eine oder andere Maßnahme als geeigneter erscheinen. Ein genereller Vergleich der verschiedenen Ansätze ist gerade nicht möglich, da die einzelnen Optionen jeweils unterschiedliche Vor- und Nachteile mit sich bringen.[578]

Bei genauer Analyse des verfolgten Zweckes liegt dieser bei einem absoluten Verschlüsselungsverbotsgesetz aber letztlich nur mittelbar in der Aufrechterhaltung staatlicher Kenntnisnahmemöglichkeiten. Unmittelbar verfolgt ein Verschlüsselungsverbot das Ziel, die Verschlüsselung von Daten zu *verhindern*.[579] Dieser Zweck kann aber tatsächlich nur im Wege eines Verschlüsselungsverbots erreicht werden. Alternativmaßnahmen zielen entweder auf die Erlangung von Schlüsseln und Passwörtern oder auf einen Datenzugriff vor der Verschlüsselung bzw. nach der Entschlüsselung. Die Verhinderung des Einsatzes von Verschlüsselungsverfahren wird allein durch ein Verschlüsselungsverbot bewirkt. Ein entsprechendes Gesetz wäre somit erforderlich.

dd) Verhältnismäßigkeit im engeren Sinne

Ein absolutes Verschlüsselungsverbotsgesetz müsste vor allem verhältnismäßig im engeren Sinne sein:

> „Die Verhältnismäßigkeit im engeren Sinne verlangt, dass die Einbußen grundrechtlich geschützter Freiheiten nicht in unangemessenem Verhältnis zu den Gemeinwohlzwecken stehen, denen die Grundrechtsbeschränkung dient. Der Gesetzgeber muss zwischen Allgemein- und Individualinteressen einen angemessenen Ausgleich herbeiführen. Dabei ist einerseits das Gewicht der Ziele und Belange zu berücksichtigen, denen der Eingriff dient. Maßgeblich ist unter anderem, wie bedeutsam die Rechtsgüter sind, die mit Hilfe der Maßnahme geschützt werden sollen, und wie wahrscheinlich der Eintritt einer Rechtsgutverletzung ist. Andererseits ist zu beachten, unter welchen Voraussetzungen welche und wie viele Grundrechtsträger wie inten-

578 So lässt sich schlicht nicht sagen, ob etwa der Einsatz von V-Leuten in gleicher Weise geeignet ist: Wurden im Umfeld verdächtigter Personen V-Leute eingesetzt, mögen diese einen vergleichbar geeigneten Ermittlungsansatz darstellen, um an Schlüssel oder Passwörter zu gelangen. Gerade im Terrorismusbereich werden aber vielfach keine V-Leute im Einsatz sein (etwa wenn es sich um unauffällig lebende sog. „Schläfer“ handelt). Für einen ganzen Deliktsbereich wäre der Einsatz von V-Leuten folglich völlig ungeeignet.

579 So auch *Meyn*, Verschlüsselung und Innere Sicherheit, S. 117.

siven Beeinträchtigungen ausgesetzt sind. Maßgebend sind insbesondere die Gestaltung der Einschreitschwellen, die Zahl der Betroffenen und die Intensität der Beeinträchtigung."[580]

Folgende Faktoren sind daher im Rahmen einer Gesamtabwägung zu berücksichtigen:

(1) Größtmögliche generelle Betroffenheit

Die Streubreite eines absoluten Verschlüsselungsverbots ist größtmöglich, da *alle* davon betroffen wären. Das BVerfG hat jüngst für die Vorratsdatenspeicherung, die ebenfalls anlassunabhängig alle Grundrechtsberechtigten betreffen würde, von einer „Streubreite, wie sie die Rechtsordnung bisher nicht kennt"[581] gesprochen. Bei Erlass eines absoluten Verschlüsselungsverbotsgesetzes wären fehlende technische Vertraulichkeit[582] der E-Mail-Kommunikation und mangelnde Anonymität beim Surfen für jedermann die allgegenwärtige Regel, nicht die individuelle Ausnahme.

(2) Umkehrung von Regel- und Ausnahmefall

Dies verkehrt die Regel-Ausnahme-Beziehung von staatlicher Freiheits- und Sicherheitsgewährleistung in ihr Gegenteil. Die Beschränkung grundrechtlicher Freiheitsrechte zur Gewährleistung von Sicherheit wird dabei vor allem deswegen als hinnehmbar angesehen, da die Einschränkungen nur im *Ausnahmefall* erfolgen, nicht im Regelfall.[583] Angesichts eines absoluten Verschlüsselungsverbotsgesetzes würde der Regelfall vertraulicher Kommunikation und anonymen Surfens aufhören zu existieren und nur noch der Ausnahmefall herrschen.

(3) Besondere Eingriffsqualität

Diese besondere Quantität der Betroffenheit wird in ihrer Bedeutung weiter erhöht durch deren Qualität: Die Grundrechtsberechtigten werden an der Verfolgung eines legitimen Anliegens gehindert, nämlich der technischen Sicherung der Vertraulichkeit ihrer (Fern-)Kommunikation. Ein Vertraulichkeitsschutz – etwa bei E-Mails –

580 BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 66 f.

581 BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 210: „Allerdings handelt es sich bei einer solchen Speicherung um einen besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt: Erfasst werden über den gesamten Zeitraum von sechs Monaten praktisch sämtliche Telekommunikationsverkehrsdaten aller Bürger ohne Anknüpfung an ein zurechenbar vorwerfbares Verhalten, eine – auch nur abstrakte – Gefährlichkeit oder sonst eine qualifizierte Situation."

582 Rechtlich ist die Vertraulichkeit dagegen unverändert durch Art. 10 I GG sowie auf einfachgesetzlicher Ebene durch § 88 TKG geschützt.

583 So *Augsberg*, Denken vom Ausnahmezustand her, in: *Arndt/Betz/Farahat/Goldmann,* Freiheit, Sicherheit, Öffentlichkeit, S. 17, 21.

wäre folglich nach heutigem Stand der Technik nicht möglich. Auch ein Schutz der Kommunikationsumstände im Internet durch anonyme Kommunikation wäre nicht möglich. Der Einzelne hat damit nur die Wahl zwischen einer in einer technischen Perspektive nicht vertraulichen Nutzung moderner Kommunikationsmedien oder einem Verzicht auf deren Nutzung. Ob ein solcher Verzicht in unserer Gesellschaft realistischerweise möglich ist oder in Zukunft sein wird, darf bezweifelt werden. Ein Verzicht wird jedenfalls zunehmend den Preis gesellschaftlicher Exklusion haben.

> „Zwar ist niemand gezwungen, das Internet für die Versendung von Nachrichten, die Abfrage von Daten, die Aufgabe von Bestellungen etc. zu benutzen, es handelt sich also nicht um Gefahrensituationen, welchen der einzelne nicht ausweichen kann. Erreicht die Nutzung des Internets jedoch eine bestimmte Qualität, die es als ein von weiten Bevölkerungsschichten genutztes, sozial übliches Mittel der Kommunikation ausweist, so wird man den Gesetzgeber für verpflichtet halten müssen, eine ‚normative Infrastruktur' zu schaffen, die Sicherheit und Vertraulichkeit im Netzverkehr gewährleistet."[584]

Hinsichtlich der Vorratsdatenspeicherung hat das BVerfG festgestellt:

> „Die Speicherung bezieht sich dabei auf Alltagshandeln, das im täglichen Miteinander elementar und für die Teilnahme am sozialen Leben in der modernen Welt nicht mehr verzichtbar ist."[585]

(4) Einschüchterungseffekte als eigenständiger Belang

In die Abwägung ebenfalls mit einzustellen ist weiter die Verunsicherung, die allein durch die *Möglichkeit* einer Überwachung von vertraulichen Gesprächen, E-Mails oder der Internetnutzung ausgelöst wird.[586] Die daraus resultierenden Einschüchte-

584 *Grote,* KritV 1999, 27, 53.

585 BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 210.

586 Dieser Verunsicherungseffekt findet Ausdruck im Verhalten der Grundrechtsberechtigten, wie eine Studie zu den Auswirkungen der Vorratsdatenspeicherung auf das Kommunikationsverhalten zeigt, vgl. Arbeitskreis Vorratsdatenspeicherung, Pressemitteilung vom 03.06. 2008, verfügbar unter: http://www.daten-speicherung.de/data/forsa_2008-06-03.pdf (04.06. 2008). Danach würde mehr als die Hälfte der befragten Personen im Hinblick auf die Vorratsdatenspeicherung nicht per Telefon oder E-Mail Kontakt mit bestimmten Einrichtungen wie Drogen- oder Eheberatungsstellen aufnehmen. Berücksichtigung finden kann aber immer nur objektiv berechtigte Furcht; andernfalls könnten alle Arten rein subjektiver, unbegründeter Ängste für alle Arten von Zwecken instrumentalisiert werden. Die staatliche Gewährleistung von „Sicherheit" in Form einer solchen „Freiheit von Furcht" kann es daher nicht geben; vgl. ausführlich dazu *Isensee*, Das Grundrecht auf Sicherheit, S. 25 f. Vgl. dazu auch die alte Idee *Benthams* des `Panopticon´, eines (Gefängnis- oder sonstigen) Bauwerks, bei dem alle Zellen/Räume jederzeit von einem zentral gelegenen Turm beobachtet werden können, ohne dass der Einzelne sehen oder wissen kann, wann er beobachtet wird und wann nicht; ausführlich siehe *Bentham*, Panopticon, in: *Bentham/Bozovic,* The Panopticon writings, S. 29.

rungseffekte fallen nach dem BVerfG ebenfalls in den grundrechtlichen Schutzbereich:[587]

> „Das Grundrecht dient dabei auch dem Schutz vor einem Einschüchterungseffekt, der entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß. Die Freiheit des Einzelnen, aus eigener Selbstbestimmung zu planen und zu entscheiden, kann dadurch wesentlich gehemmt werden. Ein von der Grundrechtsausübung abschreckender Effekt fremden Geheimwissens muss nicht nur im Interesse der betroffenen Einzelnen vermieden werden. Auch das Gemeinwohl wird hierdurch beeinträchtigt, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens ist.“[588]

(5) Wahrnehmung gewichtiger Allgemeinwohl- und Individualbelange

Diese substantiellen Eingriffe dienen wichtigen Allgemeinwohlbelangen und Individualrechtsgütern:

> „Die wirksame Strafverfolgung, die Verbrechensbekämpfung und das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren sind legitime Zwecke, die eine Einschränkung des Fernmeldegeheimnisses rechtfertigen können.“[589]

Die Aufrechterhaltung von sicherheitsbehördlichen Ermittlungsmöglichkeiten ist essentiell für die Prävention sowie die Verfolgung von Straftaten:

> „Die neuen Telekommunikationsmittel überwinden Zeit und Raum in einer mit anderen Kommunikationsformen unvergleichbaren Weise und grundsätzlich unter Ausschluss öffentlicher Wahrnehmung. Sie erleichtern damit zugleich die verdeckte Kommunikation und Aktion von Straftätern und ermöglichen es auch verstreuten Gruppen von wenigen Personen, sich zusammenzufinden und effektiv zusammenzuarbeiten. Durch die praktisch widerstandsfreie Kommunikation wird eine Bündelung von Wissen, Handlungsbereitschaft und krimineller Energie möglich, die die Gefahrenabwehr und Strafverfolgung vor neuartige Aufgaben stellt.“[590]

Durch effektive Gefahrenabwehr und Strafverfolgung werden zugleich individuelle Grundrechtspositionen aller Menschen geschützt, wie deren Recht auf Leben und körperliche Unversehrtheit (Art. 2 II S. 1 GG).[591] Des Weiteren kommt der bewirkten Sicherung des Rechtsfriedens eigenständiges Gewicht zu.

587 Vgl. etwa BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 212. *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 68 ist dagegen der Auffassung, dass der mittelbare Zwang, auf Kommunikation zu verzichten, nicht den Schutzbereich von Art. 10 GG berühre.

588 BVerfG, NJW 2007, 351, 354.

589 BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 65.

590 BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 216.

591 Siehe dazu *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, sowie unten in Teil 6.

(6) Vielfältige Umgehungsmöglichkeiten

Ein absolutes Verschlüsselungsverbot lässt sich leicht von jedem Interessierten umgehen. Letztlich wird gerade bei der Kommunikation, auf die Abhörmaßnahmen gerichtet sind, mit dem Einsatz von Verschlüsselungsverfahren zu rechnen sein.[592] Kriminelle Kreise werden sich nicht durch ein Verschlüsselungsverbot vom Schutz der Vertraulichkeit ihrer Kommunikation abhalten lassen – insbesondere, wenn diese direkt im Zusammenhang mit einer Straftat steht. Aufrecht erhalten bleibt damit im Wesentlichen die Möglichkeit, den Durchschnittsbürger abzuhören, auf den die Ermittlungsmaßnahme eigentlich gar nicht abzielt.

(7) Ungewisse Effizienz der Überwachungsmaßnahmen

Die Effizienz von Maßnahmen der Überwachung von E-Mail-Kommunikation und Internetzugängen ist ungewiss. Im Gegensatz zu Maßnahmen der Telekommunikations- und akustischen Wohnraumüberwachung, deren Effizienz im Auftrag des Bundesministeriums der Justiz wissenschaftlich untersucht wurde,[593] ist die Effizienz von E-Mail- und Internetzugangsüberwachung ungeklärt.

Seit 1997[594] wird eine jährliche Statistik über die durchgeführten Überwachungsmaßnahmen nach §§ 100a, 100 b StPO veröffentlicht.[595] Hierbei wurde bis einschließlich 2007 auch die Überwachung von Voice-over-IP-Anschlüssen[596], E-Mail-Kommunikation und Internetzugängen aufgeführt.[597] Das nunmehr[598] verant-

592 So allgemein auch *Hoffmann-Riem,* AöR 1998, 513, 519 zum Spannungsfeld von wirksamer Kriminalitätsbekämpfung und Datenschutzinteressen.

593 Hinsichtlich der TKÜ Albrecht/Dorsch/Krüpe, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, verfügbar unter: http://www.bmj.bund.de/files/-/134/Abschlussbericht.pdf (26.11.2007); hinsichtlich der akustischen Wohnraumüberwachung Meyer-Wieck, Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung („großer Lauschangriff") nach § 100c Abs. 1 Nr. 3 StPO, verfügbar unter: http://www.bmj.bund.de/files/-/786/GutachtenWohnraum%FCberwachung.pdf (26.11.2007).

594 Mit dem In-Kraft-Treten des TKG.

595 Rechtsgrundlage war zunächst § 88 V TKG, dann § 110 VIII TKG und ist jetzt § 100b V StPO. Die Statistik wurde zunächst von der Regulierungsbehörde für Telekommunikation und Post, sodann von deren Nachfolgerin, der Bundesnetzagentur, veröffentlicht. Jetzt erfüllt das Bundesamt für Justiz diese Aufgabe.

596 Dabei geht es hier zunächst um von Telekommunikationsdiensteanbietern angebotene Internettelefonie – und nicht um Fragen des Abhörens und der Abhörbarkeit von Kommunikation über Programme wie Skype, die gerade unabhängig von einem Diensteanbieter eingesetzt werden – woraus sich dann die Probleme hinsichtlich der Ende-zu-Ende-verschlüsselten Kommunikation zwischen den Kommunikationsteilnehmern ergeben.

597 In der Statistik werden nur die auf Grund der §§ 100a, 100b StPO angeordneten Überwachungsmaßnahmen erfasst. Überwachungsmaßnahmen nach § 1 I Nr. 1 G 10 oder § 23a I ZFdG werden nicht erfasst, sondern unterliegen grundsätzlich einzig der Kontrolle durch das Parlamentarische Kontrollgremium. Soweit diesbezüglich im Nachhinein Zahlen genannt werden, erscheint die Anzahl der Maßnahmen im Verhältnis vernachlässigbar (41 Anordnun-

wortliche Bundesamt für Justiz nimmt eine solche Aufschlüsselung nicht mehr vor.[599]

	Sonstige Anschlüsse/ Internetzugänge	E-Mail	VoIP-Anschlüsse
1997[600]	0	-	-
1998	3	-	-
1999	9	-	-
2000	0	-	-
2001[601]	4	0	-
2002	2	5	-
2003[602]	1	144	-
2004[603]	92	78	-
2005[604]	193	365	-
2006[605]	477	701	51
2007[606]	720	880	155
2008[607]	661[608]		

gen gem. §§ 39 ff. AWG a.F. in den Jahren 1992-2004; BT-Drs. 16/281, S. 2). Maßnahmen der Sicherstellung und Beschlagnahme von E-Mails beim Provider nach §§ 94, 98 StPO sind ebenfalls nicht erfasst (vgl. dazu BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06). Allerdings handelt es sich dabei auch nicht um Maßnahmen der (heimlichen) E-Mail-*Überwachung* – auch wenn ein großer Datenbestand Gegenstand ist.

598 Vgl. BT-Drs. 16/5846.

599 Es bleibt abzuwarten, ob weitere Zahlen – wie dies in der Vergangenheit teilweise der Fall war – in Beantwortung einer Kleinen Anfrage im Bundestag veröffentlicht werden.

600 Zahlen für die Jahre 1997 bis 2000 gem. der Jahresstatistik nach § 88 Abs. 5 TKG a.F., veröffentlicht im Tätigkeitbericht 2000/2001 der Regulierungsbehörde für Telekommunikation und Post, S. 148; verfügbar unter http://www.bundesnetzagentur.de/media/archive/206.pdf (05.05. 2008).

601 Zahlen für die Jahre 2001/2002 gem. der Jahresstatistik nach § 88 Abs. 5 TKG a.F., BT-Drs. 15/2197, S. 12.

602 Zahlen für das Jahr 2003 gem. der Jahresstatistik nach § 88 Abs. 5 TKG a.F., BT-Drs.15/4011, S. 6.

603 Zahlen für das Jahr 2004 gem. der Jahresstatistik nach § 110 Abs. 8 TKG, BT-Drs.15/6009, S. 10.

604 Zahlen für das Jahr 2005 gem. der Jahresstatistik nach § 110 Abs. 8 TKG, BT-Drs.16/2812, S. 15.

605 Zahlen für das Jahr 2006 gem. der Jahresstatistik nach § 110 Abs. 8 TKG, BT-Drs.16/6368, S. 29.

606 Zahlen für das Jahr 2007 nach heise online vom 07.05.2008, Zahl der überwachten Telefonanschlüsse stieg 2007 um 9 Prozent, verfügbar unter: http://www.heise.de/newsticker/Zahl-der-ueberwachten-Telefonanschluesse-stieg-2007-um-9-Prozent--/meldung/107545 (07.05. 2008).

607 Zahlen für das Jahr 2008 gem. der Jahresstatistik nach § 100b V StPO, verfügbar unter: http://www.bundesjustizamt.de/cln_101/nn_1635504/DE/Themen/Justizstatistik/Telekommunikatio

Die E-Mail-Überwachung wird dabei erstmals im Jahr 2001 in der Statistik genannt, die Überwachung von Voice-over-IP-Anschlüssen erstmalig im Jahr 2006. Nähere Erkenntnisse zu diesen Überwachungsmaßnahmen, etwa zu verfolgten Katalogtaten, Zahl mitbetroffener Dritter oder erzielten Ermittlungsergebnissen, wurden – soweit ersichtlich – nicht veröffentlicht. Ob die aus den Überwachungsmaßnahmen gewonnenen Erkenntnisse die mit der Überwachung von E-Mail-Kommunikation, Internetnutzung oder Internettelefonie einhergehenden massiven Grundrechtseingriffe im Sinne einer Kosten-Nutzen-Betrachtung zu rechtfertigen vermögen, ist damit einer Prüfung überhaupt nicht zugänglich.

Zwei Tendenzen können aber festgestellt werden: Erstens steigt die Quantität der Maßnahmen Internetzugangsüberwachung und E-Mail-Überwachung rasant an. Die Zunahme derartiger Überwachungsmaßnahmen spiegelt die zunehmend verbreitete Nutzung von Internet und E-Mail wieder. Das parallele Phänomen konnte in den Neunziger Jahren hinsichtlich der Mobiltelefonnutzung beobachtet werden.[609] Die Zahl der Überwachungsanordnungen ist in diesem Zeitraum sprunghaft angestiegen und scheint sich erst in den letzten Jahren auf einem (hohen) Niveau einzupendeln.[610] Daher ist sowohl hinsichtlich der Überwachung von Internetzugängen und E-Mails als auch hinsichtlich der Überwachung von Internettelefonie mit einer starken Zunahme der Überwachungsmaßnahmen zu rechnen.

Zweitens zeigt die Praxis der Telekommunikationsüberwachung nach §§ 100a, 100b StPO sowie anderer heimlicher Überwachungsmaßnahmen wie der akustischen Wohnraumüberwachung, dass die dadurch erzielten Ermittlungserfolge geringer sind als häufig suggeriert[611] wird („letztlich unverzichtbares Mittel zur Aufklärung schwer ermittelbarer Kriminalität“[612]). In Deutschland führen nur etwa 60 Prozent der Telekommunikationsüberwachungsverfahren zu einem Ermittlungserfolg,[613]

ns_C3_BCberwachung/downloads/Uebersicht__TKUE__2008,templateId=raw,property=publicationFile.pdf/Uebersicht_TKUE_2008.pdf (03.11. 2009).

608 Dies ist die Zahl der Überwachungsanordnungen für „Internettelekommunikation“, wobei nicht deutlich wird, was darunter fällt. Da die beiden weiteren Kategorien, nach denen unterschieden wird, Festnetztelekommunikation und Mobilfunktelekommunikation sind, wobei eine Überwachungsanordnung mehrere Arten zu überwachender Kommunikation umfassen kann, ist davon auszugehen, dass Internetzugangs-, E-Mail- und VoIP-Überwachung unter diese Kategorie zu subsumieren sind.

609 *Störing*, Strafprozessuale Zugriffsmöglichkeiten auf E-Mail-Kommunikation, S. 152 ff.

610 Vgl. die Zahlen aus den Jahresstatistiken nach § 88 V TKG a.F. bzw. § 110 VIII TKG n.F. *Düx,* ZRP 2003, 189, 190 nennt eine Größenordnung von 1,4 Millionen abgehörten Telefongesprächen pro Jahr.

611 So auch *Hirsch*, Bemerkungen zu den Entwürfen eines Gesetzes zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 03. März 2004, in: *Roggan,* Lauschen im Rechtsstaat, S. 87, 89.

612 BT-Drs. 16/5846, S. 23.

613 Albrecht/Dorsch/Krüpe, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, verfügbar unter: http://www.bmj.bund.de/files/-/134/Abschlussbericht.pdf (26.11.2007), S. 366 ff.

wobei es sich zum Großteil nur um mittelbare Ermittlungserfolge handelt.[614] Im Ergebnis wird etwa die Hälfte der Ermittlungsverfahren eingestellt, hauptsächlich nach § 170 Abs. 2 StPO.[615] Im Bereich der akustischen Wohnraumüberwachung wurden von 143 Verfahren nur 36 als erfolgreich oder bedingt erfolgreich eingestuft, aber 72 als nicht erfolgreich, und weitere 11 konnten gar nicht beurteilt werden.[616] Dies ist sicherlich auch der Tatsache geschuldet, dass die genannten Überwachungsmaßnahmen häufig zu Strukturermittlungen im Bereich der organisierten Kriminalität,[617] insbesondere der Drogenkriminalität, eingesetzt werden. Es beleuchtet aber recht gut das Dilemma: Strukturermittlungen umfassen zwangsläufig einen breiteren Personenkreis aufgrund eher vager Verdachtsmomente. Eine Grenzziehung, welche Maßnahmen noch verhältnismäßig sind, kann im Einzelfall schwierig sein, ist aber dringend erforderlich im Hinblick auf die massenweisen Grundrechtseingriffe. Trotz dieser rechtsstaatlichen Defizite hat sich die TKÜ

> „in den letzten Jahren `zu einem der zentralen Instrumente der Informationsbeschaffung der Sicherheitsbehörden entwickelt. Sie gilt als ein effektives und zugleich kostengünstiges Instrument der Sicherheitspolitik´. Trotz der inzwischen durch zwei empirische Studien belegten Kontrolldefizite wird die Praxis der TKÜ weiter ausgedehnt."[618]

Eine ähnliche Entwicklung für die heimliche Überwachung von Internetzugängen, E-Mail-Kommunikation und Internettelefonie kann vermutet werden, da diese Maßnahmen in ähnlichen rechtstatsächlichen Situationen und mit ähnlicher Zielsetzung durchgeführt werden dürften. Die aufgezeigten Tendenzen lassen befürchten, dass auch E-Mail-, Internetzugangs- und Internettelefonie-Überwachung unter Effizienzdefiziten leiden wird, da schwerwiegende Grundrechtseingriffe um oftmals ungewisser Ermittlungserfolge willen in Kauf genommen werden.

614 Mittelbare Ermittlungserfolge sind vor allem Hinweise auf weitere Straftaten (des Beschuldigten oder Dritter) sowie Erkenntnisse, die die Grundlage zu weiteren Ermittlungsmaßnahmen (Durchsuchungen, Vernehmungen, Einsatz verdeckter Ermittler, aber zu 50 % auch lediglich eine TKÜ bzgl. einer weiteren Nummer) bilden; vgl. Albrecht/Dorsch/Krüpe, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, verfügbar unter: http://www.bmj.bund.de/files/-/134/Abschlussbericht.pdf (26.11.2007), S. 371 ff.

615 Albrecht/Dorsch/Krüpe, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, verfügbar unter: http://www.bmj.bund.de/files/-/134/Abschlussbericht.pdf (26.11.2007), S. 344 f.

616 Zahlen nach Meyer-Wieck, Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung („großer Lauschangriff") nach § 100c Abs. 1 Nr. 3 StPO, verfügbar unter: http://www.bmj.bund.de/files/-/786/GutachtenWohnraum%FCberwachung.pdf (26.11.2007), S. 305.

617 Breyer, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, verfügbar unter: http://publikationen.ub.uni-frankfurt.de/volltexte/2005/500/pdf/BreyerPatrick.pdf (21.04.2008), S. 26.

618 *Kutscha/Roggan*, Große Lauschangriffe im Polizeirecht, in: *Roggan,* Lauschen im Rechtsstaat, S. 25, 41.

(8) Alternative Ermittlungsansätze

Im Rahmen der Verhältnismäßigkeit im engeren Sinne sind auch alternative Ermittlungsmöglichkeiten zu berücksichtigen, soweit diese geringere Grundrechtseingriffe für die Betroffenen bedeuten würden. Die Frage nach möglichen alternativen Ermittlungsansätzen lässt sich aber jeweils nur für den Einzelfall beantworten. Für spezifische Ermittlungssituationen stellen E-Mail-, Internetzugangs- und Telekommunikationsüberwachung unersetzliche Instrumente dar. Alternative Ermittlungsansätze können folglich Überwachungsmaßnahmen im Einzelfall, nicht aber generell unverhältnismäßig werden lassen.

(9) Kenntnisnahmemöglichkeiten trotz Verschlüsselung

Dabei stellt sich weiter die Frage, inwieweit der Einsatz von Verschlüsselungsverfahren tatsächlich zu einer Vereitelung der inhaltlichen Kenntnisnahme durch die staatlichen Sicherheitsbehörden führt. Angesichts der Interdependenz der Sicherheit der einzelnen Komponenten innerhalb eines IT-Sicherheitskonzepts kann vermutet werden, dass bei einem technisch durchschnittlich versierten privaten Nutzer eine inhaltliche Kenntnisnahme nicht vereitelt würde, da sein IT-Sicherheitskonzept Sicherheitslücken aufweisen würde[619] – eine Annahme, die im Kern auch dem Konzept der Online-Durchsuchung zugrunde liegt. Anders könnte dies natürlich bei professionellen Anwendern und gerade auch im kriminellen Bereich aussehen. Die Kenntnisnahme staatlicher Sicherheitsbehörden wäre aber nicht mehr kostengünstig – so dass einer der zentralen Gründe[620] für den verbreiteten Einsatz von Überwachungsmaßnahmen (zumindest hinsichtlich der Telekommunikationsüberwachung) entfiele.

(10) Abwägung

Ein absolutes Verschlüsselungsverbotsgesetz weist eine außerordentlich hohe Eingriffsqualität wie –quantität auf. Es handelt sich um den denkbar massivsten Eingriff in das Fernmeldegeheimnis: *Allen* Grundrechtsberechtigten wird *ausnahmslos* die eigenständige technische Vertraulichkeitssicherung ihrer Daten untersagt. Dem steht zwar der Schutz bedeutender Gemeinwohlinteressen gegenüber. Diese Gemeinwohlinteressen werden aber mit einem ineffektiven Ermittlungsinstrumentarium verfolgt. Weniger eingriffsintensive Maßnahmen zur Zweckerreichung sind möglich.

Daher besteht ein nicht hinnehmbares Missverhältnis zwischen der Sicherheit, die durch ein absolutes Verschlüsselungsverbot erreicht werden kann (Umgehungsmög-

619 Vergleiche die bei *Andrzejak*, Kryptoregulierung, in: *Hoeren/Queck,* Rechtsfragen der Informationsgesellschaft, S. 132, 141 f. dargestellten Erfahrungen aus den USA.

620 So *Kutscha/Roggan*, Große Lauschangriffe im Polizeirecht, in: *Roggan,* Lauschen im Rechtsstaat, S. 25, 41.

lichkeiten ohne durchgreifende Sanktionierungsoptionen für all diejenigen, die staatliche Kenntnisnahme fürchten müssen) und der Freiheit, die dafür geopfert würde (Freiheit aller, ihr Fernmeldegeheimnis vor der Kenntnisnahme Dritter effektiv zu schützen, wo der Staat keinen adäquaten Schutz bieten kann). Ein Verschlüsselungsverbot wäre daher nach hier vertretener Auffassung unverhältnismäßig.[621]

> „Zumindest aber dürfte eine derartige Kryptoregulierung unverhältnismäßig im engeren Sinne sein, denn der schmale `Erfolg´ einer Beschränkung der Handlungsmöglichkeiten bestimmter Personen, die die innere und äußere Sicherheit der Bundesrepublik gefährden, müsste mit einem außerordentlich hohen Preis erkauft werden."[622]

4. Ergebnis

Ein absolutes Verschlüsselungsverbotsgesetz würde einen Eingriff in das Fernmeldegeheimnis darstellen, der bei der gegenwärtigen Sachlage verfassungsrechtlich nicht zu rechtfertigen ist. Ein absolutes Verschlüsselungsverbotsgesetz würde zum einen gegen die Wesensgehaltsgarantie (Art. 19 II GG) verstoßen. Darüber hinaus stünde eine solche Regelung angesichts der massiven Grundrechtseingriffe, die dadurch gegenüber jedermann bewirkt würden, außer Verhältnis zu den angestrebten Zwecken der inneren und äußeren Sicherheit.

II. Verstoß gegen das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 I GG)

Ein absolutes Verschlüsselungsverbotsgesetz könnte des Weiteren – bei Daten, die sich innerhalb der Wohnung des Betroffenen befinden – einen Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 I GG darstellen.

1. Schutzbereich des Grundrechts auf Unverletzlichkeit der Wohnung (Art. 13 I GG)

a. Daten in der räumlichen Privatsphäre

Art. 13 I GG schützt mit der „Wohnung" eine räumliche Sphäre der Privatheit als Mittelpunkt der menschlichen Existenz.[623]

> „Damit wird dem Einzelnen im Hinblick auf seine Menschenwürde und im Interesse der freien Entfaltung der Persönlichkeit ein elementarer Lebensraum gewährleistet. In seinen Wohnräu-

621 So auch *Koch,* CR 1997, 106, 110; *Marauhn,* KritV 1999, 57, 81 sowie *Meyn*, Verschlüsselung und Innere Sicherheit, S. 118 ff., der zwar sachlich Art. 5 GG für einschlägig hält, inhaltlich auf der Ebene des Verhältnismäßigkeitsgrundsatzes aber dieselben Fragen prüft.

622 *Marauhn,* KritV 1999, 57, 79 zur Berufsfreiheit unter paralleler Argumentation.

623 *Gornig*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 13, Rn. 1; *Schulze-Fielitz*, in: *Dreier,* GG, Art. 2 II, Rn. 12; *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 48.

men hat er das Recht, in Ruhe gelassen zu werden. Art. 13 Abs. 1 GG gewährt ein Abwehrrecht zum Schutz der räumlichen Privatsphäre und soll Störungen vom privaten Leben fernhalten."[624]

Diese Sphäre umfasst auch die Beherrschung von Informationen über Vorgänge und Gegenstände in der Wohnung.[625] Damit schützt das Grundrecht auf Unverletzlichkeit der Wohnung auch die Vertraulichkeit von Kommunikation (unter Anwesenden), soweit sie innerhalb von Wohnungen im Sinne des Art. 13 I GG stattfindet.[626] Der Wohnungsbegriff des Art. 13 I GG ist dabei weit zu verstehen und umfasst jeden Raum,

"den ein Mensch zur Stätte seines Aufenthalts und Wirkens macht und der unbeschränkten Zugänglichkeit entzieht".[627]

Dieser räumliche Privatbereich umfasst grundsätzlich auch die Daten, die sich in dieser Sphäre befinden. Dringt der Staat physisch – im Wege der klassischen Durchsuchung (Art. 13 II GG; § 103 StPO) – oder auf andere Weise – im Wege der akustischen oder optischen Informationserhebung (sog. Lausch- bzw. Spähangriff: Art. 13 III-VI GG; §§ 100a-f StPO) – in diese räumliche Privatsphäre ein, liegt ein Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung vor.[628]

„Die heutigen technischen Gegebenheiten erlauben es, in die räumliche Sphäre auch auf andere Weise einzudringen. Der Schutzzweck der Grundrechtsnorm würde vereitelt, wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel, auch wenn sie von außerhalb der Wohnung eingesetzt werden, nicht von der Gewährleistung des Absatzes 1 umfasst wäre."[629]

b. Grenzen der räumlichen Privatsphäre

Es ist aber zunehmend umstritten, wo die durch Art. 13 I GG geschützte räumliche Privatsphäre endet. Während teilweise am traditionellen Angrenzungskriterium einer räumlichen Abschottung festgehalten wird (aa), sehen andere den Raumbezug als Äquivalent zu und Ausdruck von „ Kernbereichsrelevanz" an, so dass bei Auflösung räumlicher Abgrenzungsoptionen die Kernbereichsrelevanz maßgeblich sei (bb). Das BVerfG sieht den Schutzbereich nur bei einem hinreichenden Raumbezug als eröffnet an (cc).

624 BVerfG, Urteil vom 02.03.2006, Az.: 2 BvR 2099/04, Rn. 114.
625 *Schulze-Fielitz*, in: *Dreier,* GG, Art. 2 II, Rn. 12, 33.
626 Werden aus der durch Art. 13 I GG geschützten Sphäre Informationen erhoben, gelten lt. *Hermes*, in: *Dreier,* GG, Art. 13, Rn. 33 „die Grundsätze des Rechts auf informationelle Selbstbestimmung wie auch ihre Konkretisierungen in Bezug auf Art. 10 GG hier entsprechend."
627 *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 49.
628 *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 157.
629 BVerfG, Urteil vom 03.03.2004, Az.: 1 BvR 2378/98 und 1084/99, Rn. 105.

aa) Abschottung des geschützten Raumes

Die Grenzziehung ergibt sich grundsätzlich daraus, dass der Grundrechtsberechtigte durch „ein Mindestmaß an physischer und informationeller Abschottung des geschützten Raumes nach außen“[630] seinen Willen dokumentiert, diesen Raum der Privatheit zu widmen.[631] Ist eine derartige Grenzziehung bei realen Räumlichkeiten relativ eindeutig möglich, verkompliziert sich die Lage bei virtuellen Räumen. So wurde zum Teil argumentiert, dass ein Nutzer, der mit seinem Rechner eine Internetverbindung aufbaut, seine Privatsphäre nach außen geöffnet habe und so ein Eindringen überhaupt erst ermögliche.[632] Diese Auffassung übersieht, dass durch den Einsatz von Firewalls oder gerade auch Verschlüsselungsverfahren durchaus eine Abschottung gegen ein virtuelles Eindringen in den Rechner von außen erreicht werden kann.[633]

Die zu Grunde liegende Annahme, der Schutzbereich des Art. 13 I GG sei nur dann betroffen, wenn die Überwindung räumlicher Barrieren für ein Eindringen erforderlich ist,[634] wird der umfassenden Veränderung der gesellschaftlichen Lebenswirklichkeit durch die zunehmende Verbreitung von Informations- und Kommunikationstechnologien nicht gerecht. Im Zuge des so genannten `*internet of things*´ wird es in Zukunft in jeder Wohnung viele – smarte – Gegenstände geben, die nach dieser Logik nicht mehr vom Schutzbereich des Grundrechts auf Unverletzlichkeit der Wohnung umfasst wären, etwa Mobiltelefone, PDAs, Navigationsgeräte, Waren mit RFID-Chips, alle Arten von „intelligenten“ Gegenständen etc.[635] Die von diesen Gegenständen erfassten Informationen geben aber gleichwohl über Vorgänge und Verhaltensweisen innerhalb der räumlichen Privatsphäre der Wohnung Aufschluss.[636] Der Wohnungsbegriff kann daher nicht mehr allein über die Abschottung mittels räumlicher Barrieren definiert werden.[637]

630 *Hermes*, in: *Dreier,* GG, Art. 13, Rn. 16.

631 *Hermes*, in: *Dreier,* GG, Art. 13, Rn. 16 ff.; *Gornig*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 13, Rn. 14 ff.

632 Lorentz, NRW-LT-Stellungnahme 14/639, S. 6; Schwarz, NRW-LT-Stellungnahme 14/650, S. 6; *Hofmann,* NStZ 2005, 121, 124.

633 So *Rux,* JZ 2007, 285, 292; Sokol, NRW-LT-Stellungnahme 14/625, S. 10.

634 So *Böckenförde*, Die Ermittlung im Netz, S. 219; *Gercke,* CR 2007, 245, 250.

635 Zum sog. Pervasive oder Ubiquitous Computing siehe *Mattern,* InfSpekt 2001, 145; TAUCIS, Technikfolgenabschätzungsstudie Ubiquitäres Computing, verfügbar unter: http://www.taucis.hu-berlin.de/_download/TAUCIS_Studie.pdf (25.09.2008). Einen Eindruck eines zukünftigen „vernetzten Heims“ bietet heise online vom 11.01.2009, Fotorahmen, Wecker und Kaffeemaschine fürs vernetzte Heim, verfügbar unter: http://www.heise.de/newsticker/Fotorahmen-Wecker-und-Kaffeemaschine-fuers-vernetzte-Heim--/meldung/121511 (12.01.2009).

636 Siehe ausführlich zu technischen Möglichkeiten und deren Auswirkungen auf die Privatsphäre *Langheinrich*, Gibt es in einer total informatisierten Welt noch eine Privatsphäre?, in: *Mattern,* Die Informatisierung des Alltags, S. 233 sowie *Roßnagel*, Informationelle Selbstbestimmung in der Welt des Ubiquitous Computing, in: *Mattern,* Die Informatisierung des Alltags, S. 265.

637 *Hornung,* DuD 2007, 575, 578; so auch jüngst LG Hamburg, Beschluss vom 01.10.2007, Az.: 629 Qs 29/07, MMR 423, 424. Für einen raumbezogenen Schutz dagegen *Lepsius*, Das Com-

bb) Kernbereichsrelevanz

Im Übrigen ist keine überzeugende Begründung dafür ersichtlich, einen in der Wohnung befindlichen Brief in Papierform anders zu behandeln als eine auf dem in der Wohnung befindlichen Privatrechner gespeicherte E-Mail.[638] Der private Rechner innerhalb der durch Art. 13 I GG geschützten Wohnung ist dabei nicht weniger, sondern auf Grund der Vielzahl der enthaltenen privaten Informationen (private Videos und Fotos, E-Mails, tagebuchartige private Aufzeichnungen, Rechnungen, Konto- und Steuerdaten, in Zukunft eventuell auch Gesundheitsdaten etc.)[639] in besonderem Maße schutzbedürftig. Aus Sicht des Grundrechtsberechtigten befinden sich diese Daten, wenn sie auf einem privaten Rechner innerhalb der Wohnung gespeichert sind, sicherlich innerhalb seiner räumlichen Privatsphäre:[640]

> „Es wäre geradezu widersinnig, diesem den Grundrechtsschutz gerade dort zu versagen, wo er neuen Ermittlungsmaßnahmen ausgesetzt ist, die technisch so ausgefeilt sind, das die Mauern der Wohnung keinen Schutz bieten. Dies würde nicht nur den Schutzbereich vom technischen Fortschritt abhängig machen, sondern ihn auch kontinuierlich reduzieren."[641]

Der innerhalb der räumlichen Privatsphäre der Wohnung im Sinne des Art. 13 I GG befindliche private Rechner und die darauf gespeicherten Daten müssen daher vom Schutzbereich umfasst sein.[642] Damit kommt es – entgegen einem vielfach vorgebrachten Argument[643] – gerade auf den Standort des Speichermediums an. Dies entspricht dem Umgang mit sonstigen Gegenständen; auch diese nehmen am Schutz des Art. 13 I GG teil, soweit sie sich in einer geschützten Wohnung befinden und verlieren den Schutz, soweit sie sich nicht mehr innerhalb eines geschützten Raumes befinden.[644]

puter-Grundrecht: Herleitung – Funktion – Überzeugungskraft, in: *Roggan,* Online-Durchsuchungen, S. 21, 25, der allerdings den Schutz des Art. 13 GG allein darauf gerichtet sieht, „in Ruhe" gelassen zu werden, und daher Kommunikation auszunehmen scheint.

638 So Sokol, NRW-LT-Stellungnahme 14/625, S. 10; *Rux,* JZ 2007, 285, 293.

639 Vergleiche die Aufzählung bei *Hornung,* DuD 2007, 575, 577 sowie *Beukelmann,* StraFo 2008, 1, 1.

640 Sokol, NRW-LT-Stellungnahme 14/625, S. 10; *Rux,* JZ 2007, 285, 293; *Buermeyer,* HRRS 2007, 329, 333; *Beukelmann,* StraFo 2008, 1 ,4.

641 *Hornung,* DuD 2007, 575, 578.

642 „Entscheidend für den Eingriff in den von staatlichem Zugriff freien „elementaren Lebensraum" ist vielmehr, dass sich die Daten innerhalb eines solchen Bereichs befinden und aus ihm heraus erhoben werden, sodass die Wohnung insoweit ihren Charakter als staatsfreien Rückzugsraum des Einzelnen verliert. Die Daten auf einem Rechner innerhalb einer Wohnung sind nicht etwa nur *partiell* gegen das Mitnehmen der Hardware im Rahmen einer Hausdurchsuchung geschützt, sondern umfassend gegen jede Form auch nicht physischen staatlichen Zugriffs."; *Buermeyer,* HRRS 2007, 329, 333; ebenso *Schaar/Landwehr,* K&R 2007, 202, 204; Huster, NRW-LT-Stellungnahme 14/641, S. 4; *Hornung,* DuD 2007, 575, 578; *Hansen/Pfitzmann/Roßnagel,* DRiZ 2007, 225, 230.

643 *Hofmann,* NStZ 2005, 121, 124; Lorentz, NRW-LT-Stellungnahme 14/639, S. 6; Gusy, NRW-LT-Stellungnahme 14/629, S. 6.

644 So auch *Buermeyer,* HRRS 2007, 329, 334.

Für diese Auffassung spricht weiter, dass die Wohnung in Art. 13 I GG nicht um ihrer selbst willen, sondern als räumliche Manifestierung der höchstpersönlichen Lebenssphäre geschützt wird. In teleologischer Auslegung ergibt sich daraus, dass zur Bestimmung des Schutzbereichs von Art. 13 I GG nicht nach der räumlichen Abschottung sondern nach der Kernbereichsrelevanz gefragt werden muss.[645]

> „Übereinstimmung herrscht auch noch insoweit, als *nicht* die Räume der Wohnung *als Räume* absoluten Schutz verdienen, sondern als der Ort, an dem das absolut zu schützende *Verhalten* der „höchstpersönlichen Lebensgestaltung" sich ungestört vollziehen kann. Die Unverletzlichkeit der Wohnung ermöglicht und vermittelt die als Ausdruck der Menschenwürde *absolut* zu schützende höchstpersönliche Persönlichkeitsentfaltung."[646]

Daraus ergeben sich im Fall von gespeicherten Daten sicherlich weitreichendere Abgrenzungsprobleme als bei körperlichen Gegenständen, deren Standort einfach bestimmt werden kann und auf die auch nur körperlich zugegriffen werden kann. In der Praxis werden bei Ungewissheit über den Standort des Speichermediums nach dieser Auffassung im Zweifel auch die Anforderungen zu erfüllen sein, die Art. 13 GG an derartige Eingriffe stellt.[647]

cc) Schutzbereichsreduktion auf standortrelevante Maßnahmen?

Das BVerfG sieht demgegenüber den Schutzbereich von Art. 13 I GG nicht als eröffnet an, wenn es um den Schutz eines informationstechnischen Systems vor – standortunabhängiger – Infiltration geht:

> „Art. 13 Abs. 1 GG vermittelt dem Einzelnen allerdings keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems, auch wenn sich dieses System in einer Wohnung befindet. Denn der Eingriff kann unabhängig vom Standort erfolgen, so dass ein raumbezogener Schutz nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren."[648]

Für die Qualifizierung einer Maßnahme als Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung ist nach Auffassung des BVerfG ein irgendwie gearteter

645 So auch *Beukelmann,* StraFo 2008, 1, 4. Ist der Kernbereich privater Lebensgestaltung betroffen, muss nach *Bergemann*, Die Telekommunikationsüberwachung nach der Entscheidung des Bundesverfassungsgerichts zum "großen Lauschangriff", in: *Roggan,* Lauschen im Rechtsstaat, S. 69, 75 sogar zwangsläufig ein Gleichlauf von Art. 13 I GG und Art. 10 I GG vorliegen, da der jeweilige dort verortete Kernbereichsschutz Ausdruck des Menschenwürdegehalts der Vorschriften ist. Es handelt sich also um Konkretisierungen von Art. 1 I GG. Diese können im Rahmen von Art. 13 I GG nicht anders beurteilt werden als im Rahmen von Art. 10 I GG.

646 *Denninger*, Der "große Lauschangriff" auf dem Prüfstand der Verfassung, in: *Roggan,* Lauschen im Rechtsstaat, S. 13, 15.

647 *Hornung,* DuD 2007, 575, 278; *Buermeyer,* HRRS 2007, 329, 334; praktisch bedeutsam wird dies nur beim Zugriff von außen via Internet, im Übrigen wird der Standort des Speichermediums immer offensichtlich sein.

648 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 194.

Raumbezug erforderlich. Einen solchen Raumbezug sieht das BVerfG etwa in folgen Konstellationen noch als gegeben an:[649]

- akustische und optische Wohnraumüberwachung
- Messung elektromagnetischer Abstrahlungen eines informationstechnischen Systems
- physisches Eindringen in eine Wohnung zur Manipulation eines dort befindlichen informationstechnischen Systems
- Nutzung eines in der Wohnung vorhandenen informationstechnischen Systems zu Überwachungszwecken etwa via Mikrofon oder Kamera

Spielt der Standort des informationstechnischen Systems für die Durchführung einer Maßnahme keinerlei Rolle, ist nach Ansicht des BVerfG die räumliche Privatsphäre nicht berührt und der Schutzbereich von Art. 13 I GG nicht eröffnet:

> „Soweit die Infiltration die Verbindung des betroffenen Rechners zu einem Rechnernetzwerk ausnutzt, lässt sie die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt. Der Standort des Systems wird in vielen Fällen für die Ermittlungsmaßnahme ohne Belang und oftmals für die Behörde nicht einmal erkennbar sein. Dies gilt insbesondere für mobile informationstechnische Systeme wie etwa Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone. Art. 13 Abs. 1 GG schützt zudem nicht gegen die durch die Infiltration des Systems ermöglichte Erhebung von Daten, die sich im Arbeitsspeicher oder auf den Speichermedien eines informationstechnischen Systems befinden, das in einer Wohnung steht.“[650]

Diese Kategorisierung kann nicht gewichtiger sein als die Tatsache, dass ein in einer Wohnung befindlicher Rechner an dieser räumlichen Privatsphäre teilhat. Auf welche Weise Daten aus dieser räumlichen Privatsphäre heraus erhoben werden, kann nach hier vertretener Auffassung und entgegen der Rechtsprechung des BVerfG - jedenfalls auf Schutzbereichsebene[651] – keine Rolle spielen.[652]

c. Telekommunikation und räumliche Privatsphäre

Auch die in einer Wohnung stattfindende Telekommunikation hat grundsätzlich Teil an der räumlichen Privatsphäre. Das Verhältnis des Schutzes durch das Fernmeldegeheimnis (Art. 10 I GG) zum Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 I GG) ist daher zu konturieren:

- Wird die aus der durch Art. 13 I GG geschützten Wohnung heraus stattfindende Telekommunikation unter Ausnutzung der fernmeldetechnischen Übermittlung

649 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn.. 192 f.
650 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 194 f.
651 Für die hier vertretene, vom BVerfG abweichende Auffassung spricht, dass das BVerfG bei der Ablehnung der Eröffnung des Schutzbereichs dogmatisch wenig überzeugend bereits mit dem (vermeintlichen) Fehlen eines Eingriffs argumentiert. Dabei ist zunächst der grundrechtliche Schutzbereich zu konturieren und dann daran gemessen zu beurteilen, ob ein Eingriff vorliegt.
652 So auch *Hornung,* CR 2008, 299, 301.

abgehört, ist nur der Schutzbereich des Fernmeldegeheimnisses betroffen.[653] Ein darüber hinausgehender Eingriff in die Integrität der Wohnung, der in den Schutzbereich des Art. 13 I GG fallen würde, liegt nicht vor.

- Werden dagegen Telekommunikationsverbindungen oder Abhöreinrichtungen in Telefonen auch zum Abhören von sonstigen Gesprächen innerhalb der Wohnung genutzt, liegt daneben auch ein Eingriff in Art. 13 I GG vor.[654] Wegen der unterschiedlichen Anknüpfungsmerkmale des Kommunikationsmediums im Rahmen von Art. 10 I GG einerseits und der räumlichen Sphäre bei Art. 13 I GG andererseits sind tatbestandliche Überschneidungen im Übrigen nicht denkbar.[655]

Soweit der Einsatz von Verschlüsselungstechnologien allein dem Schutz der Vertraulichkeit der Telekommunikation dient, ist daher Art. 10 I GG das spezielle Grundrecht und allein maßgeblich. Der Schutz des Fernmeldegeheimnisses endet nach der Rechtsprechung des BVerfG dann, wenn die übermittelten Daten oder sonstigen Inhalte endgültig in die Herrschaftssphäre des Kommunikationsteilnehmers gelangen – da sie dann nicht mehr den spezifischen Kenntnisnahmegefahren der fernmeldetechnischen Übermittlung ausgesetzt sind, für die das Fernmeldegeheimnis einen rechtlichen Ausgleich bietet:[656]

> „Ohne dass es in diesem Zusammenhang auf die wandelbaren Einzelheiten der Löschbarkeit digital gespeicherter Daten ankäme, hat der Nutzer in seiner Herrschaftssphäre Möglichkeiten der Datenverarbeitung und –löschung – bis hin zur physischen Zerstörung des Datenträgers –, die ihm nicht zu Gebote stehen, solange sich die Nachricht auf dem Übertragungsweg befindet oder die Kommunikationsverbindungsdaten beim Nachrichtenmittler gespeichert sind. Der Nutzer kann sich bei den seiner Verfügungsmacht unterliegenden Geräten gegen unerwünschten Zugriff Dritter durch vielfältige Maßnahmen schützen, etwa durch die Benutzung von Passwörtern oder anderweitiger Zugangscodes sowie – bei Verwendung von Personalcomputern – durch Einsatz von Verschlüsselungsprogrammen und spezieller Software zur Datenlöschung."[657]

Nach Beendigung des Telekommunikationsvorgangs werden die Daten genauso behandelt wie alle sonstigen privaten Daten. Soweit diese sich auf dem heimischen Rechner oder sonstigen Datenträgern innerhalb der Wohnung befinden, ist der Schutzbereich des Art. 13 I GG eröffnet.

> „Die nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Kommunikationsverbindungsdaten werden jedoch nicht durch Art. 10 Abs. 1 GG, sondern durch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1

653 *Gurlit,* RdV 2006, 43, 44.

654 *Gurlit,* RdV 2006, 43, 44; *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 101; *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 97.

655 *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 101.

656 Für E-Mails, die dauerhaft in einem zugangsgesicherten E-Mail-Postfach beim Provider gespeichert sind, bedeutet dies nach der jüngst getroffenen Entscheidung des BVerfG (Beschluss vom 16.06.2009, Az.: 2 BvR 902/06), dass der Kommunikationsvorgang noch nicht endgültig abgeschlossen und damit der Schutzbereich des Fernmeldegeheimnisses weiterhin eröffnet ist.

657 BVerfG, Urteil vom 02.03.2006, Az.: 2 BvR 2099/04, Rn. 80.

in Verbindung mit Art. 1 Abs. 1 GG) und gegebenenfalls durch Art. 13 Abs. 1 GG geschützt."[658]

d. Gewährleistung des Einsatzes von Verschlüsselungsverfahren durch Art. 13 I GG

Das Grundrecht auf Unverletzlichkeit der Wohnung umfasst auch den Einsatz von Verschlüsselungsverfahren zum Schutz der innerhalb der räumlichen Privatsphäre befindlichen Daten. Dabei kann im Wesentlichen parallel zu den im Rahmen des Fernmeldegeheimnisses dargestellten Aspekten argumentiert werden: Verschlüsselung dient der Verwirklichung des räumlichen Privatsphärenschutzes. Wie die Diskussion um die Online-Durchsuchung[659] eindrücklich zeigt, existieren vielfältige Möglichkeiten, auf die Daten zuzugreifen, die sich auf einem Rechner mit Internetanbindung befinden. Daher stellt die Nutzung von Verschlüsselungsverfahren ein notwendiges und adäquates Mittel zum technischen Selbstschutz des Einzelnen dar. Unabhängig davon, ob es nach dem Urteil des BVerfG zur Online-Durchsuchung[660] in Zukunft verfassungsgemäße Rechtsgrundlagen für die heimliche Durchsuchung privater Rechner geben wird,[661] sehen sich Internetnutzer in jedem Fall den Angriffen interessierter Dritter ausgesetzt. Verschlüsselungstechnologien sind zentrale Elemente sicherer IT-Systeme, um sich gegen das Ausspähen von Daten zu schützen. Daher muss der durch Art. 13 I GG vermittelte Schutz der räumlichen Privatsphäre auch den Einsatz von Verschlüsselungsverfahrens umfassen.

2. Grundrechtseingriff durch ein absolutes Verschlüsselungsverbot

Ein absolutes Verschlüsselungsverbotsgesetz würde daher nach hier vertretener, vom BVerfG abweichender Auffassung einen Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 I GG darstellen.

658 BVerfG, Urteil vom 02.03.2006, Az.: 2 BvR 2099/04, Rn. 72.

659 Zu der Frage, ob es sich beim heimlichen Zugriff auf Daten, die sich auf dem heimischen PC befinden, um eine „Durchsuchung" im Sinne des Art. 13 II GG bzw. des § 102 StPO handelt, vergleiche *Hofmann,* NStZ 2005, 121, 123 f.; *Gercke,* CR 2007, 245, 250; *Rux,* JZ 2007, 285, 292 f. Zu der in vielen Punkten parallelen Diskussion, ob der Große bzw. Kleine Lauschangriff als „akustische Durchsuchung" anzusehen sei vergleiche *Gornig*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 13, Rn. 66.

660 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07.

661 Siehe oben am Anfang des Kapitels. Aus anderen strafprozessualen Rechtgrundlagen ergibt sich laut BGH, Beschluss vom 31.01.2007, Az.: StB 18/06, K&R 2007, 158 jedenfalls keine Befugnis zu einer Online-Durchsuchung.

3. Verfassungsrechtliche Rechtfertigung eines absoluten Verschlüsselungsverbots

Der Grundrechtseingriff durch ein absolutes Verschlüsselungsverbotsgesetz könnte verfassungsrechtlich gerechtfertigt sein. Dabei normiert Art. 13 GG je nach Eingriffsmaßnahme unterschiedliche Schrankenregelungen. Da ein absolutes Verschlüsselungsverbotsgesetz weder eine Durchsuchung nach Art. 13 II GG noch eine Überwachungsmaßnahme mit technischen Mitteln gem. Art. 13 III-V GG darstellt, könnte ein solches Verbotsgesetz allenfalls nach Art. 13 VII GG verfassungsrechtlich gerechtfertigt sein, der die Schrankenregelungen für sonstige „Eingriffe und Beschränkungen" normiert.[662] Aber auch danach ist ein absolutes Verschlüsselungsverbot nicht zu rechtfertigen. Art. 13 VII GG ermöglicht Eingriffe zur Gefahrenabwehr.[663] Ein absolutes Verschlüsselungsverbot ist aber eine Dauermaßnahme, keine punktuelle Gefahrenabwehrmaßnahme. Selbst wenn man im Hinblick auf den Begriff der „Verhütung" dringender Gefahren auch Maßnahmen unter Art. 13 VII GG subsumieren will, die dem Zweck dienen, „einen Zustand nicht eintreten zu lassen, der seinerseits eine dringende Gefahr für die öffentliche Sicherheit und Ordnung darstellen würde",[664] kann dies eine auf Dauer angelegte Maßnahme nicht rechtfertigen.

Der Eingriff in Art. 13 I GG ist nach dessen differenzierter Schrankensystematik nicht zu rechtfertigen, da ein Verschlüsselungsverbotsgesetz unter keine der Schrankenregelungen in Art. 13 II-V, VII GG fällt. Zwar spricht die potentielle Kernbereichsrelevanz – und damit der Menschenwürdegehalt – von Daten in der räumlichen Privatsphäre[665] auch für einen Verstoß gegen die Wesensgehaltsgarantie (Art. 19 II GG), da ein Verschlüsselungsverbotsgesetz es dem Einzelnen unmöglich machen würde, Daten innerhalb seiner räumlichen Privatsphäre gegen Ausspähung zu schützen. Angesichts der zunehmenden Digitalisierung und Vernetzung auch der häuslichen Privatsphäre und ihrer Durchdringung mit immer mehr `smarten´ Gegenständen dürfte darin ein Verstoß gegen die Wesensgehaltsgarantie liegen.[666] Darüber

662 Unter „Eingriffe und Beschränkungen" im Sinne des Art. 13 VII GG sind alle Eingriffe in den Schutzbereich von Art. 13 I GG zu subsumieren, die nicht Durchsuchung nach Art. 13 II GG oder Überwachungsmaßnahme nach Art. 13 III-V GG sind; *Gornig*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 13, Rn. 148; *Hermes*, in: *Dreier,* GG, Art. 13, Rn. 105.

663 *Gornig*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 13, Rn. 155, 158; *Hermes*, in: *Dreier,* GG, Art. 13, Rn. 111.

664 *Gornig*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 13, Rn. 158.

665 S.o. unter 1.b.bb). Vgl. auch BVerfG, Urteil vom 03.03.2004, Az.: 1 BvR 2378/98 und 1 BvR 1084/99, Rn. 119: „Der Schutz der Menschenwürde wird auch in dem Grundrecht aus Art. 13 Abs. 1 GG konkretisiert. Die Unverletzlichkeit der Wohnung hat einen engen Bezug zur Menschenwürde und steht zugleich im nahen Zusammenhang mit dem verfassungsrechtlichen Gebot unbedingter Achtung einer Sphäre des Bürgers für eine ausschließlich private – eine "höchstpersönliche" – Entfaltung. Dem Einzelnen soll das Recht, in Ruhe gelassen zu werden, gerade in seinen Wohnräumen gesichert sein."

666 So auch *Beukelmann,* StraFo 2008, 1, 4, der allerdings allein die Frage nach der Möglichkeit einer entsprechenden Verfassungsänderung, also nach dem Umfang Ewigkeitsgarantie nach Art. 79 III GG, stellt und keinen Verstoß gegen Art. 19 II GG diskutiert.

hinaus muss ein absolutes Verschlüsselungsverbotsgesetz jedenfalls an der Verhältnismäßigkeitsprüfung scheitern, wobei auf die parallele Argumentation im Rahmen des Fernmeldegeheimnisses verwiesen werden kann.

Die Bedeutung der Feststellung eines Eingriffs in Art. 13 I GG liegt aber maßgeblich darin, dass sich die Verfassungswidrigkeit eines absoluten Verschlüsselungsverbotsgesetzes – jenseits aller Abwägungsentscheidungen und schwer festzumachender Wesengsehaltserwägungen – unmittelbar aus der Schrankenregelung von Art. 13 GG ergibt. Dabei ist das Grundrecht auf Unverletzlichkeit der Wohnung, was (informations-)technologische Neuerungen angeht, zugleich das modernste und aktuellste Grundrecht – mit der umfassenden Neugestaltung der Schrankenregelung im Jahr 1998 zur Einführung von Lausch- und Spähangriff.[667] Die ausgefeilte Schrankensystematik verdeutlicht, dass für eine weite, dynamische Auslegung der Schrankenbestimmungen kein Raum ist. Eine Änderung von Art. 13 GG mit dem Ziel, durch Schaffung einer weiteren Schrankenregelung ein absolutes Verschlüsselungsverbotsgesetz zu ermöglichen, würde im Hinblick auf die Kernbereichsrelevanz gegen Art. 79 III GG verstoßen.[668]

4. Ergebnis

Ein absolutes Verschlüsselungsverbotsgesetz würde nach hier vertretener Ansicht einen Eingriff in das Recht auf Unverletzlichkeit der Wohnung (Art. 13 I GG) bedeuten, der unter keine der Schrankenregelungen der Art. 13 II-VII GG fällt und somit nicht verfassungsrechtlich zu rechtfertigen ist. Anders dagegen das BVerfG, welches den Schutzbereich von Art. 13 I GG wegen fehlenden Raumbezuges für nicht eröffnet hält.

III. Verstoß gegen das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG)

Ein absolutes Verschlüsselungsverbotsgesetz könnte darüber hinaus auch einen Eingriff in das aus Art. 2 I GG i.V.m. Art. 1 I GG abgeleitete allgemeine Persönlichkeitsrecht, insbesondere in seinen Ausprägung als Recht auf informationelle Selbstbestimmung sowie als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, darstellen.

667 Vgl. ausführlich dazu *Hermes*, in: *Dreier,* GG, Art. 13, Rn. 56 ff.
668 *Beukelmann,* StraFo 2008, 1, 4.

1. Schutzbereich des allgemeinen Persönlichkeitsrechts (Art. 2 I GG i.V.m. Art. 1 I GG)

Art. 2 I GG schützt zum einen die allgemeine Handlungsfreiheit und zum anderen – in Verbindung mit Art. 1 I GG – das allgemeine Persönlichkeitsrecht. Die allgemeine Handlungsfreiheit umfasst dabei alle Arten menschlicher Aktivität, während das allgemeine Persönlichkeitsrecht als „Recht, in Ruhe gelassen zu werden“[669] den Schutz der personalen Integrität gewährleistet.[670] Beide Aspekte zielen auf die Erhaltung von Freiheit und Autonomie.[671] Die allgemeine Handlungsfreiheit schützt dabei die Freiheit des Einzelnen, sich nach seinen Vorstellungen zu verhalten. Das allgemeine Persönlichkeitsrecht gewährleistet die Grundbedingungen, unter denen der Einzelne überhaupt in seinen Handlungen frei sein kann.[672] Innerhalb des allgemeinen Persönlichkeitsrechts kann weiter unterschieden werden zwischen dem Schutz eines privaten Rückzugsbereichs (ein „Innenraum, in dem er [der Einzelne; d. Verf.] sich selbst besitzt“[673]) einerseits und dem Schutz der persönlichen Selbstdarstellung in der Öffentlichkeit andererseits.[674]

> „Jedermann darf grundsätzlich selbst und allein bestimmen, ob und inwieweit andere sein Lebensbild im ganzen oder bestimmte Vorgänge aus seinem Leben öffentlich darstellen dürfen.“[675]

Das allgemeine Persönlichkeitsrecht als unbenanntes Freiheitsrecht ist allerdings nicht abschließend definiert und konturiert:

> „Das allgemeine Persönlichkeitsrecht ergänzt als "unbenanntes" Freiheitsrecht die speziellen ("benannten") Freiheitsrechte, die, wie etwa die Gewissens- oder die Meinungsfreiheit, ebenfalls konstituierende Elemente der Persönlichkeit schützen. Seine Aufgabe ist es, im Sinne des obersten Konstitutionsprinzips der Würde des Menschen (Art. 1 Abs. 1 GG) die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen zu gewährleisten, die sich durch die traditionellen Freiheitsgarantien nicht vollständig erfassen lassen; diese Notwendigkeit besteht namentlich auch im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen für den Schutz der menschlichen Persönlichkeit. Wegen der Eigenart des allgemeinen Persönlichkeitsrechts hat die Rechtsprechung des Bundesverfassungsgerichts den Inhalt des geschützten Rechts nicht abschließend umschrieben, sondern seine Ausprägungen jeweils anhand des zu entscheidenden Falles herausgearbeitet.“[676]

669 BVerfGE 27, 1, 6.
670 *Dreier*, in: *Dreier,* GG, Art. 2 I, Rn. 23; *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 86.
671 *Dreier*, in: *Dreier,* GG, Art. 2 I, Rn. 25; Rössler, Der Wert des Privaten, verfügbar unter: http://www.aec.at/de/festival2007/topics/d_roessler_lang.pdf (06.09.2007), S. 7 ff.
672 *Dreier*, in: *Dreier,* GG, Art. 2 I, Rn. 25.
673 BVerfGE 27, 1, 6.
674 *Dreier*, in: *Dreier,* GG, Art. 2 I, Rn. 24; *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 30 f.; *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 88; *Scholz/Pitschas*, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, S. 69.
675 BVerfGE 35, 202, 220.
676 BVerfGE 79, 256, 268.

Als Teilgehalte des allgemeinen Persönlichkeitsrechts wurden bisher etwa anerkannt:[677]

- das Recht am vertraulich gesprochenen Wort,
- das Recht an privaten Aufzeichnungen,
- das Recht am eigenen Bild,
- der Schutz davor, dass jemandem Äußerungen in den Mund gelegt werden, die er nicht getan hat und die seinen sozialen Geltungsanspruch beeinträchtigen,
- das Recht auf informationelle Selbstbestimmung und
- das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[678]

a. Recht auf Vertraulichkeit

Den Teilgehalten Recht am eigenen Wort, [679] Recht am eigenen Bild, Recht auf informationelle Selbstbestimmung[680] sowie Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[681] ist gemeinsam, dass es im Kern um die Gewährleistung von Vertraulichkeit geht. Zum einen gewährleistet Art. 2 I GG i.V.m. Art. 1 I GG einen Kernbereich privater Lebensgestaltung, der „wegen der besonderen Nähe zur Menschenwürde […] als absolut unantastbar geschützt ist.“[682] Nach der Rechtsprechung des BVerfG im Volkszählungsurteil umfasst das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung

> „[…] auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.“[683]

Der Einzelne hat somit ein Recht auf private Geheimnisse. Aber auch da, wo der Einzelne diesen höchstpersönlichen Bereich verlässt und seine Geheimnisse anderen offenbart, genießt dies den Schutz des allgemeinen Persönlichkeitsrechts. Das allgemeine Persönlichkeitsrecht umfasst auch die Befugnis, darüber zu bestimmen, wer von Gesprächsinhalten Kenntnis erhält.

677 Aufzählung im Wesentlichen nach *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 87.

678 *Lepsius*, Das Computer-Grundrecht: Herleitung – Funktion – Überzeugungskraft, in: *Roggan,* Online-Durchsuchungen, S. 21, 36 sieht das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dagegen nicht als Teilgehalt des allgemeinen Persönlichkeitsrechts an, sondern versteht dieses allein objektiv-rechtlich (siehe S. 34 ff.). Als „prozessual motivierte Rechtsposition“ (S. 37) könne es allein im Wege der allgemeinen Handlungsfreiheit als subjektive Rechtsposition geltend gemacht werden.

679 Siehe insbesondere BVerfGE 80, 367, 373 ff.

680 BVerfGE 65, 1, 42 ff.

681 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07.

682 BVerfG vom. 13.06.2007, Az: 1 BvR 1783/05, Rn. 88 (juris).

683 BVerfGE 65, 1, 42.

„Zum Grundrecht gehört die Befugnis selbst zu bestimmen, ob der Kommunikationsinhalt einzig dem Gesprächspartner, einem bestimmten Personenkreis oder der Öffentlichkeit zugänglich sein soll. Das Selbstbestimmungsrecht erstreckt sich also auf die Auswahl der Personen, die Kenntnis vom Gesprächsinhalt erhalten sollen."[684]

Geschützt wird also nicht nur ein privater Rückzugsbereich, sondern auch der kommunikative Kontakt zu anderen. Der Mensch als soziales Wesen verwirklicht sich gerade auch in seinen kommunikativen Beziehungen. Diese können auch Bestandteil des absolut geschützten Kernbereichs privater Lebensgestaltung sein:[685]

„Der Mensch als Person, auch im Kernbereich seiner Persönlichkeit, verwirklicht sich notwendig in sozialen Bezügen."[686]

Daher erscheint es wenig sinnvoll, auf Schutzbereichsebene zwischen einem Geheim- oder Intimbereich einerseits und einem Privatsphärenbereich andererseits zu unterscheiden.[687] Das allgemeine Persönlichkeitsrecht gewährleistet vielmehr umfassend ein Recht auf Vertraulichkeit,[688] sei es in der Auseinandersetzung mit sich selbst (im Selbstgespräch, durch Führen eines Tagebuchs etc.), sei es in der Kommunikation mit anderen:[689]

„Menschliche Kommunikation soll durch das Grundrecht dagegen geschützt sein, dass die Worte – eine vielleicht unbedachte oder unbeherrschte Äußerung, eine bloß vorläufige Stellungnahme im Rahmen eines sich entfaltenden Gesprächs oder eine nur aus einer besonderen Situation heraus verständliche Formulierung – bei anderer Gelegenheit und in anderem Zusammenhang hervorgeholt werden, um durch Inhalt, Ausdruck oder Klang gegen den Sprechenden zu zeugen."[690]

684 BVerfG, Beschluss vom 09.10.2002, Az.: 1 BvR 1611/96 und 805/98, Rn. 29.

685 *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 36.

686 BVerfG, Urteil vom 03.03.2004, Az.: 1 BvR 2378/98 und 1084/99, Rn. 136.

687 In Anlehnung an die aus der sphärentheoretischen Rechtsprechung des BVerfG stammenden Begriffe der Intimsphäre einerseits und Privatsphäre andererseits. Vergleiche zur Abgrenzung *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 78 f. Auch bei einem Abschied von der Differenzierung nach Privatheitssphären auf Schutzbereichsebene wird das Kriterium der Eingriffsqualität nicht obsolet, die „Qualität des Grundrechtseingriffs" wird nunmehr im Rahmen der Verhältnismäßigkeitsprüfung zu berücksichtigen sein. Dementsprechend hält *Hufen*, Schutz der Persönlichkeit und Recht auf informationelle Selbstbestimmung, in: *Badura/Dreier,* Festschrift 50 Jahre Bundesverfassungsgericht, S. 105, 114 die Verhältnismäßigkeit für den eigentlichen „Sitz der Sphärentheorie". Vgl. zur Kritik an der Sphärentheorie auch *Bizer*, Forschungsfreiheit und informationelle Selbstbestimmung, S. 146 m.w.N. Dagegen hält *Kloepfer,* Informationsrecht, § 3, Rn. 47 die Sphärentheorie durchaus für sinnvoll, soweit die Kategorisierung nicht den Blick für die Relativität der Sphären verstelle.

688 Dieses Recht auf Vertraulichkeit stimmt gerade nicht mit dem Privatsphärenschutz, wie er etwa von *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 173 verstanden wird, überein. Nach jener Konzeption beginnt der Privatsphärenschutz jenseits des Schutzbereichs der Menschenwürde, während hier keine derartige Trennung vorgenommen werden soll. Daraus rechtfertigt sich auch die abweichende Terminologie.

689 v. *Mutius*, Anonymität als Element des allgemeinen Persönlichkeitsrechts – terminologische, rechtssystematische und normstrukturelle Grundfragen, in: *Bäumler/v. Mutius,* Anonymität im Internet, S. 12, 20.

690 BVerfG, Beschluss vom 09.10.2002, Az.: 1 BvR 1611/96 und 805/98, Rn. 30.

Dies zeigt sich auch in dem jüngst vom BVerfG herausgearbeiteten Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[691] Auch hier werden nicht nur Daten geschützt, die dem Bereich der Privatsphäre zuzuordnen sind:

> „Das Schutzbedürfnis des Nutzers eines informationstechnischen Systems beschränkt sich jedoch nicht allein auf Daten, die seiner Privatsphäre zuzuordnen sind."[692]

Nach Auffassung des BVerfG ist die Privatsphärenrelevanz eines Datums weder umfassend vorherseh- noch objektivierbar.[693]

> „Eine solche Zuordnung hängt zudem häufig von dem Kontext ab, in dem die Daten entstanden sind und in den sie durch Verknüpfung mit anderen Daten gebracht werden. Dem Datum selbst ist vielfach nicht anzusehen, welche Bedeutung es für den Betroffenen hat und welche es durch Einbeziehung in andere Zusammenhänge gewinnen kann."[694]

Die Grenze der Schutzbereichserstreckung ist aber erreicht, wenn es sich um Daten mit nur punktuellem Bezug zum Grundrechtsträger handelt; hier bleibt es bei dem durch das Recht auf informationelle Selbstbestimmung gewährten Schutz, der einen Personenbezug voraussetzt.

> „Allerdings bedarf nicht jedes informationstechnische System, das personenbezogene Daten erzeugen, verarbeiten oder speichern kann, des besonderen Schutzes durch eine eigenständige persönlichkeitsrechtliche Gewährleistung. Soweit ein derartiges System nach seiner technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen enthält – zum Beispiel nicht vernetzte elektronische Steuerungsanlagen der Haustechnik -, unterscheidet sich ein staatlicher Zugriff auf den vorhandenen Datenbestand qualitativ nicht von anderen Datenerhebungen. In einem solchen Fall reicht der Schutz durch das Recht auf informationelle Selbstbestimmung aus, um die berechtigten Geheimhaltungsinteressen des Betroffenen zu wahren."[695]

b. Recht auf Integrität informationstechnischer Systeme

Neben der Vertraulichkeit wird auch die Integrität informationstechnischer Systeme geschützt. Der Integritätsschutz scheint aber nach der Entscheidung des BVerfG eher eine dienende Funktion als eigenständige Bedeutung zu haben. Die Integrität informationstechnischer Systeme wird vom BVerfG mit der Begründung geschützt, dass durch eine Integritätsbeeinträchtigung „Ausspähung, Überwachung oder Manipulation des Systems"[696] möglich werden:

> „Geschützt vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist zunächst das Interesse des Nutzers, dass die von einem vom

691 Siehe BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07.
692 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 197.
693 Vergleiche zur Unterscheidung von privaten und personenbezogenen Daten bereits *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 43.
694 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 197.
695 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 202.
696 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 204.

> Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.“[697]

Der Schutz der Integrität informationstechnischer Systeme stellt danach einen puren Annex zum Schutz der Vertraulichkeit informationstechnischer Systeme dar. Die Integrität wird nur in den Schutzbereich einbezogen, weil nach einer Integritätsbeeinträchtigung ohne weitere entscheidende technische Hürde direkt die Vertraulichkeit beeinträchtigt werden kann. Eine derartige Vorverlagerung in den Bereich reiner Rechtsgutsgefährdungen ist dem BVerfG nicht fremd. Bereits im Volkszählungsurteil führte das BVerfG für das Recht auf informationelle Selbstbestimmung aus, dass es „unter den Bedingungen der automatischen Datenverarbeitung kein `belangloses´ Datum mehr“[698] gebe. Entscheidend für die Schutzbedürftigkeit war nach Auffassung des BVerfG nicht allein die Art der Angabe, sondern vor allem die Möglichkeit, mit Hilfe der Informationstechnologie Daten zu verarbeiten und zu verknüpfen:

> „Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; […]“[699]

Bereits die Möglichkeit, dass Daten verknüpft werden *könnten*, dass daraus teilweise oder weitgehend vollständige Persönlichkeitsbilder[700] generiert werden *könnten* und dass deren eventuelles Vorhandensein wiederum den Einzelnen in seiner Freiheit „aus eigener Selbstbestimmung zu planen oder zu entscheiden“[701] hemmen *könnte*, reicht für das BVerfG aus, den Schutzbereich des Rechts auf informationelle Selbstbestimmung einerseits auf *alle* Daten auf einem informationstechnischen System zu erstrecken und andererseits bereits auf die *Schaffung der Möglichkeit zur Erhebung* des Datums vorzuverlagern, auch wenn es in der Sache hauptsächlich um den Schutz vor der Verknüpfung von Daten geht.

> „Das Recht auf informationelle Selbstbestimmung trägt Gefährdungen und Verletzungen der Persönlichkeit Rechnung, die sich für den Einzelnen, insbesondere unter den Bedingungen moderner Datenverarbeitung, aus informationsbezogenen Maßnahmen ergeben. Dieses Recht flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit; es lässt ihn schon auf der Stufe der Persönlichkeitsgefährdung beginnen.“[702]

Das Bedürfnis nach dem Schutz der Integrität informationstechnischer Systeme ist – insbesondere im Vergleich zum Zeitpunkt der Anerkennung des Rechts auf informationelle Selbstbestimmung durch das BVerfG – vor allem den folgenden Phänomenen geschuldet: Der Einzelne sieht sich heute weniger einzelnen gezielten Datenerhebungen durch den Staat gegenüber, er lebt vielmehr in einer zunehmend digi-

697 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 204.
698 BVerfGE 65, 1, 45.
699 BVerfGE 65, 1, 45.
700 BVerfGE 65, 1, 42.
701 BVerfGE 65, 1, 43.
702 BVerfG, Urteil vom 11.03.2008, Az.: 1 BvR 2074/05 und 1254/07, Rn. 63

talisierten Gesellschaft. Das bedeutet, dass der Einzelne regelmäßig auf die Nutzung informationstechnischer Systeme angewiesen ist – gerade auch zur Verwirklichung seiner freien Persönlichkeitsentfaltung. Dabei duldet der Nutzer nicht passiv eine (zwangsweise) staatliche Datenerhebung, sondern die Daten werden vom Nutzer aktiv einem informationstechnischen System anvertraut oder entstehen technisch bedingt durch die Nutzung selbst. Verzicht auf die Nutzung informationstechnischer Systeme stellt keine adäquate Lösung (mehr) dar. Den aus dieser gesellschaftlichen Realität resultierenden Persönlichkeitsgefährdungen muss durch die Gewährleistung der Integrität informationstechnischer Systeme Rechnung getragen werden.

> „Jedoch trägt das Recht auf informationelle Selbstbestimmung den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus.“[703]

Der Integritätsschutz gilt dabei sowohl für „die im Arbeitsspeicher gehaltenen als auch die temporär oder dauerhaft auf den Speichermedien des Systems abgelegten Daten“.[704] Der Schutz umfasst alle Arten von Datenerhebungen, nicht nur solche, die mittels eines informationstechnischen Systems durchgeführt werden:

> „Das Grundrecht schützt auch vor Datenerhebungen mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben. So liegt es etwa bei einem Einsatz von sogenannten Hardware-Keyloggern oder bei einer Messung der elektromagnetischen Abstrahlung von Bildschirm oder Tastatur.“[705]

Erforderlich ist aber eine berechtigte Privatheitserwartung des Nutzers:

> „Eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht allerdings nur, soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt. Soweit die Nutzung des eigenen informationstechnischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden, erstreckt sich der Schutz des Nutzers auch hierauf.“[706]

703 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 200.
704 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 205.
705 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 205.
706 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 206.

c. Recht auf Anonymität?

Das allgemeine Persönlichkeitsrecht könnte neben der Vertraulichkeit auch ein Recht auf Anonymität[707] umfassen, das anonyme elektronische Kommunikation ebenso wie anonymes Surfen im Internet gewährleistet.

Für die Anerkennung eines solchen Rechts auf Anonymität spricht, dass bei der Nutzung elektronischer Verfahren, wie etwa der Nutzung des Internets, unvermeidbar elektronische Spuren entstehen, die umfassenden Aufschluss über das Verhalten des Einzelnen geben können, wie das BVerfG jüngst in seiner Entscheidung zur Vorratsdatenspeicherung ausgeführt hat:

> „Die Aussagekraft dieser Daten ist weitreichend. Je nach Nutzung von Telekommunikationsdiensten seitens der Betroffenen lassen sich schon aus den Daten selbst – und erst recht, wenn diese als Anknüpfungspunkte für weitere Ermittlungen dienen – tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten eines jeden Bürgers gewinnen. Zwar werden mit einer Telekommunikationsverkehrsdatenspeicherung, wie in § 113a TKG vorgesehen, nur die Verbindungsdaten (Zeitpunkt, Dauer, beteiligte Anschlüsse sowie – bei der Mobiltelefonie – der Standort) festgehalten, nicht aber auch der Inhalt der Kommunikation. Auch aus diesen Daten lassen sich jedoch bei umfassender und automatisierter Auswertung bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen. Adressaten (deren Zugehörigkeit zu bestimmten Berufsgruppen, Institutionen oder Interessenverbänden oder die von ihnen angebotenen Leistungen), Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen derjenigen, deren Verbindungsdaten ausgewertet werden. Einen Vertraulichkeitsschutz gibt es insoweit nicht. Je nach Nutzung der Telekommunikation und künftig in zunehmender Dichte kann eine solche Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers ermöglichen. Bezogen auf Gruppen und Verbände erlauben die Daten überdies unter Umständen die Aufdeckung von internen Einflussstrukturen und Entscheidungsabläufen.“[708]

Der in der „realen“ Welt so selbstverständliche Zustand der Nicht-Identifizierbarkeit existiert ohne Implementierung entsprechender Schutzinstrumente bei der Nutzung von Informations- und Kommunikationsdiensten nicht.[709] Prinzipiell ist aber kein Grund ersichtlich, weswegen alltägliche Aktivitäten wie Information, Kommunikation oder Konsum, nur weil sie via Internet erfolgen, nicht anonym stattfinden sollen – ebenso wie dies in der „realen“ Welt anonym möglich ist.[710]

707 Vgl. ausführlich zu Begriff und Dimensionen von Anonymität *Brunst*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, S. 6 ff.

708 BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 211.

709 *Weichert*, in: *Däubler/Klebe/Wedde/Weichert,* BDSG, Einleitung, Rn. 49.

710 So auch *Brunst*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, S. 259. Dem entspricht, dass laut *Bäumler*, Das Recht auf Anonymität, in: *Bäumler/v. Mutius,* Anonymität im Internet, S. 1, 3 auf einfachgesetzlicher Ebene Anonymität die Regel, die Identifizierung hingegen der Ausnahmefall ist. Zur individuellen als auch kollektiven Bedeutung von Anonymität als sozialem Phänomen siehe ausführlich *Brunst*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, S. 9 ff.

Informationelle Selbstbestimmung wird am wirksamsten dadurch gewährleistet, dass personenbezogene Daten erst gar nicht generiert werden. Dem entsprechen auf einfachgesetzlicher Ebene die datenschutzrechtliche Gebote der Datensparsamkeit und der Datenvermeidung (§ 3a BDSG). Der Gesetzgeber scheint dies ähnlich zu werten, da mit dem Informations- und Kommunikationsdienste-Gesetz (IuKDG)[711] die gesetzliche Verpflichtung für Anbieter von Telediensten geschaffen wurde, den Nutzern, soweit möglich und zumutbar, die anonyme oder pseudonyme[712] Nutzung der Dienste zu ermöglichen.[713] Eine identische Regelung findet sich nunmehr auch in § 13 VI des am 01.03.2007 in Kraft getretenen Telemediengesetzes.[714]

Schließlich schützt das Recht auf informationelle Selbstbestimmung Kommunikationsumstände (um die es bei Fragen der Anonymität im Kern geht) ebenso wie Kommunikationsinhalte; entscheidend ist allein der personale Bezug. Daher ist ein Recht auf Anonymität als eigenständiger Teilgehalt des allgemeinen Persönlichkeitsrechts anzuerkennen.[715]

d. Recht auf Verschlüsselung?

Zur Verwirklichung der Rechte auf Vertraulichkeit, Integrität und Anonymität könnte aus dem allgemeinen Persönlichkeitsrecht ein Recht auf Verschlüsselung zu deduzieren sein. Sowohl Vertraulichkeit als auch Integrität und Anonymität werden technisch durch den Einsatz von Verschlüsselungstechnologien erreicht. Verschlüsselungsverfahren setzen technisch um, was grundrechtlich durch das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) gewährleistet wird. Der Einzelne muss berechtigt sein, seine grundrechtlich gewährleisteten Rechtspositionen aus dem allgemeinen Persönlichkeitsrecht auf diesem Weg selbst effektiv zu schützen. Dafür spricht die immer breiter werdende Schere zwischen zunehmenden Gefähr-

711 Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste vom 22.07.1997, BGBl. I 1997, 1870.

712 Pseudomisierung ist technisch und rechtlich kein eigenständiges Schutzziel, sondern stets Mittel zur (weitgehenden) Erreichung von Anonymität, vgl. oben in Teil 1 unter B.III.1.a.dd). Daher wird hier auch nur ein Recht auf Anonymität und nicht daneben auch ein eigenständiges Recht auf Pseudonymität erörtert; ein Recht auf Pseudonymität folgt zwanglos aus und ist begründet durch ein Recht auf Anonymität. Vgl. ausführlich zu Pseudonymität *Brunst*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, S. 27 ff.

713 Vergleiche § 4 I TDDSG a.F.: „Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren."

714 Telemediengesetz vom 26.02.2007, BGBl. I 2007, 179.

715 So auch *Weichert*, in: *Däubler/Klebe/Wedde/Weichert,* BDSG, Einleitung, Rn. 50; v. *Mutius*, Anonymität als Element des allgemeinen Persönlichkeitsrechts – terminologische, rechtssystematische und normstrukturelle Grundfragen, in: *Bäumler/v. Mutius,* Anonymität im Internet, S. 12, ; a.A. ohne nähere Begründung *Dreier*, in: *Dreier,* GG, Art. 2 I, Rn. 87; *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 87.

dungen des Einzelnen durch die fortschreitende Digitalisierung und abnehmender (national-)staatlicher Steuerungs- und Schutzfunktion:

aa) Wachsende Digitalisierung

Der Einzelne sieht sich einer veränderten Gefährdungsintensität ausgesetzt, die sich insbesondere aus dem Zusammenspiel der folgenden sieben Faktoren ergibt:[716]

(1) Verlagerung von Alltagsgeschäften

Die Nutzung von Informations- und Kommunikationstechnologien nimmt gerade auch bei Alltagsaktivitäten einen immer breiteren Raum ein. Es kann insoweit eine Verlagerung beobachtet werden: Aktivitäten, die früher in der „realen" Welt stattgefunden haben, werden heute zunehmend auf elektronischem Weg verwirklicht.[717]

(2) Steigende Betroffenheit sensibler Daten

Dabei sind nicht nur immer mehr, sondern vor allem auch in immer stärkerem Maß sensible Daten (§ 3 IX BDSG)[718] des Einzelnen sowie Daten, die sonstigen besonderen Vertraulichkeitsschutz genießen, involviert: Gesundheitsdaten werden auf der elektronischen Gesundheitskarte gespeichert, Bankgeschäfte werden online erledigt, Behörden- oder Gerichtskontakte werden zunehmend durch E-Government- bzw. E-Justice-Anwendungen ersetzt, Steuerdaten elektronisch an das Finanzamt übermittelt etc.[719]

(3) Permanenz von Daten

Dadurch kann ein „stilles" Wissen generiert werden, was früher so überhaupt nicht vorhanden war. So weiß in der „realen" Welt heute niemand mehr, welche Bücher jemand vor fünf Jahren gekauft hat, während ein Online-Buchhändler solche für ihn

716 Vergleiche dazu insgesamt auch BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 170-180.

717 Vergleiche BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 174; v. *Bonin*, Die Kontrolle digitaler Kommunikationsinhalte, S. 105 sowie *Brunst*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, S. 257 ff. und 280 f.

718 Die „besonderen Arten personenbezogener Daten" nach § 3 IX BDSG werden zum Teil als sensible, zum Teil als sensitive Daten bezeichnet. Ein inhaltlicher Unterschied scheint mit der unterschiedlichen Terminologie nicht verbunden zu sein.

719 Zu den auf einem privaten Rechner vorhandenen Daten siehe auch *Beukelmann,* StraFo 2008, 1, 1.

interessanten Kundeninformationen durchaus speichert. Anonymität ist nicht nur immer seltener möglich, es gibt auch kein digitales „Vergessen“.

(4) Verkettbarkeit von Daten

Hinsichtlich jedes Einzelnen existieren also nicht nur immer mehr Daten aus immer mehr Bereichen, diese bieten auch immer mehr Möglichkeiten, die Daten miteinander zu verketten und so neue Informationen zu generieren.[720]

(5) Zunehmende Sozialüblichkeit

Zudem ist zu konstatieren, dass sich der Einzelne diesen Virtualisierungstendenzen immer weniger entziehen kann, ohne dass dies Mechanismen gesellschaftlicher Exklusion bedingen würde:

> "Je stärker das Internet das tägliche Leben mitbestimmt, desto stärker hängen die Freiheitschancen des einzelnen vom Zugang zum Internet ab."[721]

(6) Verbesserte Auswertungsmöglichkeiten

Schließlich können nicht nur immer mehr Daten erfasst und gespeichert werden, vorhandene Daten können mit neuen Suchfunktionen und Filterverfahren auch immer besser ausgewertet werden.[722]

(7) Qualifizierte Angriffsszenarien

Zuletzt ist festzustellen, dass immer mehr und immer qualifiziertere Angriffe auf Daten stattfinden, aus höchst unterschiedlichen Motiven (finanzielle Interessen, Geltungsdrang, Experimentierfreude, Neugier oder auch ideelle Motive, um nur einige zu nennen[723]). Sobald ein privater PC über einen Internetzugang verfügt, besteht grundsätzlich die Gefahr widerrechtlichen Eindringens und unbefugter Kenntnis-

720 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 175 sowie Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 211; vergleiche zum Problemkomplex der Verkettung digitaler Identitäten Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Verkettung digitaler Identitäten, verfügbar unter: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf (05.11.2007).

721 *Kube*, in: *Isensee/Kirchhof,* HStR IV, § 91, Rn. 6.

722 Vgl. etwa die Ausführungen bei heise online vom 15.11.2007, Wirtschaftsministerium sieht wenig Änderungsbedarf bei der Providerhaftung, verfügbar unter: http://www.heise.de/newsticker/meldung/99070 (16.11.2007); so auch BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 172.

723 Vgl. insoweit nur Wikipedia, Hacker, Version vom 27.08.2009, 14.34 Uhr, verfügbar unter: http://de.wikipedia.org/wiki/Hacker.

nahme durch Dritte. Dabei gilt auch für den Bereich der Schadsoftware: Es sind immer weniger Fachkenntnisse notwendig;[724] daraus folgt, dass immer mehr Menschen das Werkzeug Schadsoftware nutzen können.

Aus dem Zusammenwirken dieser Einzelfaktoren ergibt sich für den Einzelnen ein verschärftes Gefährdungspotential.

bb) Zunehmende staatliche Schutzdefizite

Demgegenüber stehen dem Staat immer weniger tatsächliche Handlungsspielräume offen, um diesem erhöhten Bedrohungsszenario wirksam zu begegnen. Die Implementierung technischer Schutzmaßnahmen ist von staatlicher Seite ohnehin nicht möglich.[725] Ein rechtliches Verbot des Ausspähens (§ 202a I StGB) oder Abfangens von Daten (§ 202b StGB), von Datenveränderung (§ 303a I StGB) und Computersabotage (§ 303b I StGB) kann tatsächlich keinen effektiven Schutz vor derartigen Angriffen bewirken. Der Nationalstaat mit seiner begrenzten Jurisdiktionshoheit kann den angesichts der Internationalität der Netze vielfach grenzüberschreitenden Sachverhalten nicht wirksam begegnen:[726]

> "Die Netze konstituieren einen neuen *körperlosen Sozialraum*. Auf diesen werden zunehmend mehr soziale Kontakte, wirtschaftlicher Austausch und rechtlicher Verkehr übertragen. In ihm herrschen andere Bedingungen als in den Sozialbeziehungen der körperlichen Welt. In dieser neuen Welt hat der Staat kein Zwangsmittel, kein Gewaltmonopol und keine Souveränität."[727]

Selbst bei erfolgreicher transnationaler Harmonisierung von Straftatbeständen sowie Abschluss multilateraler Rechtshilfe-, Vollstreckungs- und Auslieferungsübereinkommen kann dennoch prognostiziert werden, dass Derartiges nicht auf globaler Ebene unter Einbeziehung aller Staaten gelingen wird, da die einzelstaatlichen Interessen stark divergieren.[728] Es kann vielmehr gemutmaßt werden, dass es immer Staaten geben wird, die entweder kein Interesse an der effektiven Ermittlung, Verfolgung und Durchsetzung international harmonisierter Strafrechtsnormen haben oder aber rein faktisch dazu nicht in der Lage sind.

724 Vgl. heise online vom 10.06.2008, Trojanerbaukasten mit Rund-um-die-Uhr-Support und Austausch-Service, verfügbar unter: http://www.heise.de/newsticker/Trojanerbaukasten-mit-Rund-um-die-Uhr-Support-und-Austausch-Service--/meldung/109254 (11.06.2008).

725 *Roßnagel,* ZRP 1997, 26, 27.

726 Siehe zu den Problemen der Strafverfolgung bei Auslandsbezug *Bär,* CR 1995, 158-169, 227-234, 232.

727 *Roßnagel,* ZRP 1997, 26, 28.

728 Divergenzen können sich dabei nicht nur aus dem vorherrschenden nationalstaatlichen Paradigma des Vorrangs nationaler Interessen ergeben, sondern auch schlicht aus unterschiedlichen rechtshistorischen Erfahrungen und Prägungen der verschiedenen Rechtsordnungen: was nach unserer Rechtstradition und nach unserem Rechtsverständnis eine strafbare sog. „Auschwitz-Lüge" ist (§ 130 III StGB), sieht ein US-Amerikaner als zulässige Meinungsäußerung an.

Daher wird es aller Voraussicht nach immer „Oasen“ geben, von denen aus Kriminelle (weitgehend) unbehelligt operieren können. Solchen Rechtsdurchsetzungsmängeln auf globaler Ebene kommt im virtuellen Raum deshalb besondere Bedeutung zu, da es für Kriminelle schon ausreichen kann, Provider in Ländern mit Rechtsdurchsetzungsdefiziten zu nutzen, um ihre Identität wirksam zu verschleiern – selbst wenn Verschlüsselung, Anonymisierung und Steganographie in Deutschland verboten wären.[729]

cc) Konsequenz: Ermöglichung privaten Selbstschutzes

Da der Staat, wie soeben dargestellt, mit dem ihm zu Gebote stehenden Instrumentarium den Einzelnen nicht (mehr) wirksam schützen kann, muss er ihm zumindest gestatten, sich selbst zu schützen:

> „Wenn der demokratische Rechtsstaat seine Bürger im neuen Sozialraum der Netze nicht mehr zuverlässig schützen kann, muß er sie zum Ausgleich zum Selbstschutz befähigen.“[730]

Alles andere hieße, den Einzelnen angesichts eines vielfach potenzierten Bedrohungsszenarios de facto rechtlos zu stellen. Art. 2 I GG i.V.m. Art. 1 I GG muss daher auch die Befugnis des Einzelnen beinhalten, sein Recht auf Vertraulichkeit, sein Recht auf Integrität und sein Recht auf Anonymität selbst durch technische Schutzmaßnahmen zu sichern.[731] Das allgemeine Persönlichkeitsrecht gewährleistet somit ein Recht auf Verschlüsselung.

> „Sind die Bürger in der Informationsgesellschaft auf kommunikative Selbstentfaltung und folglich informationellen Austausch angewiesen, kann es dem Grundrecht auf informationelle Selbstbestimmung beispielsweise nicht entsprechen, wenn der Staat diese Entfaltungsmöglichkeit durch intensive Regelung auch dort beschränkt oder gar unterbindet, wo die Bürger sich selbst schützen können.“[732]

e. Verhältnis der Teilgehalte zueinander

Das Verhältnis der einzelnen Teilgehalte des allgemeinen Persönlichkeitsrechts (Art. 2 I GG i.V.m. Art. 1 I GG) ist dabei wenig konturiert.

Für die Abgrenzung der beiden hier zentralen Teilgehalte – das Recht auf informationelle Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – ist nach der Rechtsprechung des BVerfG entscheidend, ob der Eingriff „Einblick in wesentliche Teile der Lebensge-

729 Bei Nutzung dieser technischen Optionen wäre eine Identitätsverschleierung auch ohne Weiteres im Inland möglich; so für ein Verbot von Anonymisierungsdiensten auch *Möller,* DuD 2000, 267, 271.

730 *Roßnagel,* ZRP 1997, 26, 29.

731 So auch die Argumentation von *Roßnagel,* ZRP 1997, 26, 29.

732 *Hoffmann-Riem,* AöR 1998, 513, 531.

staltung“ erlaubt bzw. ein „aussagekräftiges Bild der Persönlichkeit“ gewonnen werden kann:

> „Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ist hingegen anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer, einerlei ob sie fest installiert oder mobil betrieben werden. Nicht nur bei einer Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung lässt sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen. Der spezifische Grundrechtsschutz erstreckt sich ferner beispielsweise auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können.“[733]

Das einzelne personenbezogene Datum ist also durch das Recht auf informationelle Selbstbestimmung geschützt, eine Datenansammlung – in einem Personalcomputer, Mobiltelefon oder PDA[734] – durch das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Dabei wird eine durch das Recht auf Gewährleistung der Vertraulichkeit und Integrität geschützte Datenansammlung häufig personenbezogene Daten beinhalten, die bereits durch das Recht auf informationelle Selbstbestimmung geschützt sind. Der Schutz des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geht aber über den durch das Recht auf informationelle Selbstbestimmung vermittelten Schutz hinaus:

- *Zum einen inhaltlich hinsichtlich der geschützten Daten*: Da die Privatsphärenrelevanz eines Datums nach der Rechtsprechung des BVerfG weder umfassend vorherseh- oder objektivierbar ist,[735] schützt das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme *alle Daten* auf einem solchen System – *unabhängig von Personenbezug oder Privatsphärenrelevanz*.[736]
- *Zum anderen zeitlich-funktional hinsichtlich des Beginns des grundrechtlichen Schutzes*: Während das Recht auf informationelle Selbstbestimmung an die tatsächlich erfolgende Erhebung oder Verarbeitung von Daten anknüpft, ist der Schutzbereich des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (weiter) *vorverlagert auf den Zeitpunkt der*

733 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 203.

734 Siehe zu den besonderen Herausforderungen, die sich in Zukunft durch die zunehmende Nutzung vernetzter Systeme ergeben werden Hansen/Pfitzmann, Windei Bundestrojaner, verfügbar unter: http://www.heise.de/ct/artikel/Windei-Bundestrojaner-291808.html (10.11.2009).

735 Vgl. BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 197 sowie oben unter a.

736 Das Recht auf informationelle Selbstbestimmung schützt Daten mit *Personenbezug*. Der Begriff der *Privatsphärenrelevanz* ist demgegenüber weiter und erfasst auch Daten ohne Personenbezug.

Erhebungsmöglichkeit. Diese ist nach der Rechtsprechung des BVerfG gegeben, wenn Dritte so auf das System zugreifen können, dass sie dessen „Leistungen, Funktionen und Speicherinhalte“ [737] nutzen können. Denn damit sei „die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.“[738]

Die Schutzbereiche des Rechts auf informationelle Selbstbestimmung und des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme *überschneiden sich also bei der Erhebung personenbezogener Daten aus informationstechnischen Systemen, die „Einblick in wesentliche Teile der Lebensgestaltung“ erlauben bzw. ein „aussagekräftiges Bild der Persönlichkeit“ geben.*

Datenerhebungen jenseits derartiger informationstechnischer Systeme sind allein vom Recht auf informationelle Selbstbestimmung erfasst. Daten auf informationstechnischen Systemen, die keinen Personenbezug bzw. keine Privatsphärenrelevanz aufweisen, sind allein durch das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geschützt. Dieser Schutz beginnt bereits mit der Infiltration[739] des informationstechnischen Systems. Daraus ergibt sich folgende Matrix:[740]

	innerhalb eines IT-Systems[741]		außerhalb eines IT-Systems	
	ohne Personenbezug	Personenbezug	Personenbezug	ohne Personenbezug
Erhebung	IT	IT / inf.S.	inf.S.	-
Infiltration	IT	IT	-	-

Bei gleichzeitiger Eröffnung der Schutzbereiche des Rechts auf informationelle Selbstbestimmung und des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme scheint das BVerfG[742] auch insoweit[743] von

737 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 204.

738 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 204.

739 Zum Begriff der Infiltration siehe *Hansen/Pfitzmann*, Techniken der Online-Durchsuchung: Gebrauch, Missbrauch, Empfehlungen, in: *Roggan,* Online-Durchsuchungen, S. 131, 133 ff.

740 Das Recht auf Gewährleistung der Integrität und Vertraulichkeit wird in Anlehnung an die teilweise verwendete Bezeichnung als IT-Grundrecht hier mit IT abgekürzt, das Recht auf informationelle Selbstbestimmung mit inf.S.

741 Gemeint ist natürlich ein informationstechnisches System, das Einblicke in wesentliche Teile der Lebensgestaltung erlaubt bzw. ein aussagekräftiges Bild der Persönlichkeit gibt.

742 In seiner jüngsten, zweiten Entscheidung zum Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme: BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06.

743 Die ebenfalls bestehende Subsidiarität gegenüber Art. 10 GG und Art. 13 GG spiegelt ohnehin die ständige Rechtsprechung des BVerfG wieder und ist auch in der Literatur allgemein anerkannt.

der Subsidiarität des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auszugehen:

> „[…] ist nicht am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG zu messen. Dieses schützt vor Eingriffen in informationstechnische Systeme nur, soweit der Schutz nicht durch andere Grundrechte, insbesondere Art. 10 oder Art. 13 GG, sowie das Recht auf informationelle Selbstbestimmung gewährleistet ist."[744]

Die Annahme eines Subsidiaritätsverhältnisses beschreibt das Zusammenspiel der beiden Ausprägungen des allgemeinen Persönlichkeitsrechts allerdings nicht zutreffend: Eine Datenansammlung – Abgrenzungskriterium hinsichtlich einer Schutzbereichseröffnung des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – besteht denknotwendig aus einzelnen (in der Regel auch personenbezogenen) Daten, die durch das Recht auf informationelle Selbstbestimmung geschützt sind. Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist mithin nicht subsidiär gegenüber dem Recht auf informationelle Selbstbestimmung, sondern setzt vielmehr (regelmäßig) seine Betroffenheit voraus.[745] Insofern könnte man eher von einem Spezialitätsverhältnis sprechen. Da aber nicht alle Einzelangaben, die durch das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geschützt werden, zwingend personenbezogen sein müssen, kann nicht in jedem Fall von einem Spezialitätsverhältnis gesprochen werden.

In Abweichung von der sich herauskristallisierenden Auffassung des BVerfG werden die Teilgehalte „Recht auf informationelle Selbstbestimmung" und „Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" als Ausprägungen ein und desselben Grundrechts, des allgemeinen Persönlichkeitsrechts (Art. 2 I GG i.V.m. Art. 1 I GG), verstanden und nicht als eigenständige, trennscharf gegeneinander abgrenzbare Grundrechte.[746] Dies entspricht auch dem status quo bezüglich weiterer Teilgehalte: So handelt es sich bei den Teilgehalten des Rechts am eigenen Bild und des Rechts an eigenen Aufzeichnungen[747] etwa denknotwendig immer auch um personenbezogene Daten, ist also auch der Teilgehalt des Rechts auf informationelle Selbstbestimmung betroffen. Die Teilgehalte

744 BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 51.

745 Dementsprechend hat *Lepsius*, Das Computer-Grundrecht: Herleitung – Funktion – Überzeugungskraft, in: *Roggan,* Online-Durchsuchungen, S. 21, 29 ff. darauf hingewiesen, dass die Feststellung der Verfassungswidrigkeit der nordrhein-westfälischen Rechtsgrundlage für die Online-Durchsuchung auch auf das Recht auf informationelle Selbstbestimmung hätte gestützt werden können.

746 So im Ergebnis auch *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 27 f., der die Offenheit, Flexibilität und Anpassungsfähigkeit des Privatsphärenschutzes hinsichtlich neuer Entwicklungen und Gefährdungssituationen betont. Vgl. dazu auch *Roßnagel/Schnabel,* NJW 2008, 3534, 3534; zu den insbes. hinsichtlich des Rechts auf informationelle Selbstbestimmung vertretenen Positionen vgl. *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 49 m.w.N.

747 Klassifiziert nach *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 95.

sind eben keine eigenständigen Rechte, sondern Ausprägungen oder Aspekte desselben Muttergrundrechts, des allgemeinen Persönlichkeitsrechts.[748]

Eine Abgrenzung der Teilgehalte ist weder möglich noch – angesichts gemeinsamer Schranken – nötig. Daher wird auch hier das allgemeine Persönlichkeitsrecht in seiner Gänze erörtert, wobei jeweils einzelne Teilgehalte eine herausgehobene Rolle spielen mögen. Dies ändert aber nichts an deren grundsätzlicher Verankerung und Zugehörigkeit zum allgemeinen Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG).

Dem entsprechend wird im Weiteren immer vom allgemeinen Persönlichkeitsrecht die Rede sein, da zumeist mehrere Teilgehalte betroffen sind oder betroffen sein können (etwa bei Daten auf einem informationstechnischen System: das Recht auf informationelle Selbstbestimmung, das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, das Recht am eigenen Bild, das Recht am eigenen Wort, das Recht an privaten Aufzeichnungen). Im Sinne der Lesbarkeit wird daher auf eine Aufzählung der (möglicherweise) betroffenen Teilgehalte verzichtet und allgemein das allgemeine Persönlichkeitsrecht genannt. Zentral sind dabei natürlich stets das Recht auf informationelle Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, deren Schutzbereiche bereits konturiert wurden. Nur wenn ausnahmsweise nur einer der Teilgehalte betroffen ist oder in besonders herausgehobener Weise betroffen ist, wird dieser explizit genannt.

f. Verhältnis zu anderen Grundrechten

aa) Fernmeldegeheimnis (Art. 10 I GG)

Zu prüfen ist, wie sich das aus dem allgemeinen Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) ableitbare Recht auf Verschlüsselung zum Recht auf Verschlüsselung aus dem Fernmeldegeheimnis (Art. 10 I GG) verhält. Da das Recht auf Verschlüsselung im Bereich des Fernmeldegeheimnisses der Verwirklichung dieses Grundrechts dient, gelten schlicht die allgemeinen Grundsätze des Grundrechtsschutzes aus Art. 10 I GG, und zwar auch im Hinblick auf die Schutzbereichsabgrenzung: Ist der Schutzbereich des Fernmeldegeheimnisses eröffnet, dann ist das Grundrecht aus Art. 10 I GG gegenüber dem Grundrecht des allgemeinen Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) speziell und somit vorrangig.[749] Dies

748 Daher wurde hier das Recht auf informationelle Selbstbestimmung – auch wenn es schon fast eigenständigen Charakter gewonnen hat und vielfach nicht mehr als Ausprägung des allgemeinen Persönlichkeitsrechts wahrgenommen wird – auch nur im Rahmen des allgemeinen Persönlichkeitsrechts und nicht in einem eigenen Abschnitt erörtert.

749 *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 94; *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 103; vergleiche dazu auch ausführlich *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 236 ff. mit grundlegenden Erwägungen zum Verhältnis des allgemeinen Privatsphären-

gilt auch für die durch die Rechtsprechung herausgearbeiteten Ausprägungen des allgemeinen Persönlichkeitsrechts wie das Recht auf informationelle Selbstbestimmung.[750]

Art. 10 I GG schützt Inhalt und Umstände von mit Hilfe von Telekommunikationstechniken übermittelten Informationen.[751] Beginn und Ende des Übermittlungsvorgangs markieren Beginn und Ende des Schutzbereichs des Fernmeldegeheimnisses. Dabei sind Beginn und Ende des Übermittlungsvorgangs allerdings nicht rein technisch zu bestimmen, sondern im Wege einer juristischen Wertung zu ermitteln.

(1) Zeitliche Grenze: Beginn des durch das Fernmeldegeheimnis vermittelten Schutzes

Soweit ersichtlich ist bisher der Zeitpunkt des Beginns des Schutzes des Fernmeldegeheimnisses nicht näher diskutiert worden. Dieser beginnt grundsätzlich mit dem Zeitpunkt des Beginns des Übermittlungsvorgangs, so wie dieser technisch determiniert ist. Ein diesem Zeitpunkt vorgelagerter Schutz wurde nur hinsichtlich des Einsatzes des so genannten `*IMSI-Catchers´*[752] diskutiert.[753] Der `*IMSI-Catcher´* simuliert die Existenz der Basisstation eines Mobilfunknetzes. Alle Mobiltelefone in Reichweite der simulierten Funkzelle buchen sich bei der vermeintlichen Funkzelle ein. Der `*IMSI-Catcher´* fragt dann die IMSI oder auch die IMEI (`*International Mobile Equipment Identity´*), die international einmalige Gerätenummer des Mobiltelefons, ab. Nach Auffassung des BVerfG ist aber der Schutz des Fernmeldegeheimnisses nicht auf den Zustand der Kommunikationsbereitschaft vorzuverlagern. Nach Ansicht des BVerfG handelt es sich um technische Signale ohne hinreichenden Telekommunikationsbezug:

> „Beim Einsatz des `IMSI-Catchers´ `kommunizieren´ ausschließlich technische Geräte miteinander. Es fehlt an einem menschlich veranlassten Informationsaustausch, der sich auf Kommunikationsinhalte bezieht."[754]

Die eventuell vorhandenen Auswirkungen auf die Kommunikationsbereitschaft der Grundrechtsträger durch Einschüchterungseffekte sind nach der Rechtsprechung des BVerfG nicht an Art. 10 I GG zu messen, da nicht die Bedingungen freier Telekommunikation an sich eingeschränkt werden.[755]

schutzes aus Art. 2 I GG (i.V.m. Art. 1 I GG) zum speziellen Privatsphärenschutz etwa aus Art. 10 I GG, Art. 13 I GG, aber auch aus Art. 4, 5, 6, 8, 9 GG.

750 *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 94; *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 103.

751 Siehe oben unter I.1.a.bb)(2).

752 Die IMSI (`*International Mobile Subscriber Identity´*) ist die weltweit einmalig vergeben Kartennummer (SIM – `*Subcriber Identity Mobile´*) zum Betrieb eines Mobiltelefons.

753 *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 53, 72 m.w.N.

754 BVerfG, Beschluss vom 22.08.2006, Az.: 2 BvR 1345/03, Rn. 57.

755 BVerfG, Beschluss vom 22.08.2006, Az.: 2 BvR 1345/03, Rn. 59.

„[…] die vorgelagerte Kommunikationsanbahnung [verdient] nicht den gleichen Schutz."[756]

Nach hier vertretener Auffassung ist der Schutzbereich des Fernmeldegeheimnisses jedenfalls zeitlich auf den Verschlüsselungsvorgang vorzuverlagern, wenn es um die Verschlüsselung von Daten geht, die dann unter Einsatz von Telekommunikationstechniken übermittelt werden sollen.[757] Im Übrigen bleibt es bei der Eröffnung des Geltungsbereichs des Fernmeldegeheimnisses ab dem Zeitpunkt des technischen Übermittlungsbeginns.

(2) Zeitliche Grenze: Ende des durch das Fernmeldegeheimnis vermittelten Schutzes

Grundsätzlich endet der Schutz des Art. 10 I GG mit dem Empfang der Nachricht und dem (technischen) Ende des Übertragungsvorgangs:

„Der Schutz des Fernmeldegeheimnisses endet insoweit in dem Moment, in dem die Nachricht bei dem Empfänger angekommen und der Übertragungsvorgang beendet ist."[758]

Wann der Übermittlungsvorgang bei E-Mails in diesem Sinne beendet ist, war dabei vor allem für die Fälle umstritten, in denen die E-Mails vom Empfänger nicht auf seinen eigenen Computer (oder PDA, Mobiltelefon etc.) heruntergeladen werden, sondern dieser seine E-Mails – ob gelesen oder ungelesen – dauerhaft auf dem Server seines Providers belässt.[759] Das BVerfG hat nunmehr entschieden, dass – wegen der fortdauernden besonderen Kenntnisnahmegefahren, die die Betroffenheit des Fernmeldegeheimnisses charakterisieren – der Übermittlungsvorgang *in einer juristischen Bewertung nicht abgeschlossen* ist:

„Der Schutz des Fernmeldegeheimnisses endet insoweit in dem Moment, in dem die E-Mail beim Empfänger angekommen und der Übertragungsvorgang beendet ist. Demgegenüber ist der zugangsgesicherte Kommunikationsinhalt in einem E-Mail-Postfach, auf das der Nutzer nur über eine Internetverbindung zugreifen kann, durch Art. 10 Abs. 1 GG geschützt. Das Fernmeldegeheimnis knüpft an das Kommunikationsmedium an und will jenen Gefahren für die Vertraulichkeit begegnen, die sich gerade aus der Verwendung dieses Mediums ergeben, das einem staatlichem Zugriff leichter ausgesetzt ist als die direkte Kommunikation unter Anwesenden."[760]

Dementsprechend fallen E-Mails so lange in den Schutzbereich des Fernmeldegeheimnisses, bis sie *endgültig* im Herrschaftsbereich des Empfängers angekommen sind, d.h. in der Regel erst nach dem Herunterladen der Mails auf den eigenen Rechner bei gleichzeitiger Löschung auf dem Server des E-Mail-Providers. Das BVerfG stellt maßgeblich auf die *faktische Herrschaft* über die Daten ab:

756 BVerfG, Beschluss vom 22.08.2006, Az.: 2 BvR 1345/03, Rn. 61.

757 Siehe oben unter I.1.b. Anders dagegen *Meyn*, Verschlüsselung und Innere Sicherheit, S. 57, der den Schutzbereich von Art. 10 I GG erst in dem Moment als eröffnet ansieht „in dem die Nachricht sich eben nicht mehr im alleinigen Machtbereich des Berechtigten befindet".

758 BVerfG, Urteil vom 02.03.2006, Az.: 2 BvR 2099/04, Rn. 73.

759 Vergleiche ausführlich zum Streitstand *Schlegel,* HRRS 2007, 44 sowie in einer vor allem strafprozessualen Betrachtung *Böckenförde*, Die Ermittlung im Netz, S. 390 ff.

760 BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 45 f.

„Die auf dem Mailserver des Providers vorhandenen E-Mails sind nicht im Herrschaftsbereich des Kommunikationsteilnehmers, sondern des Providers gespeichert. Sie befinden sich nicht auf in den Räumen des Nutzers verwahrten oder in seinen Endgeräten installierten Datenträgern. Der Nutzer kann sie für sich auf einem Bildschirm nur lesbar machen, indem er eine Internetverbindung zum Mailserver des Providers herstellt. Zwar kann der Nutzer versuchen, die auf dem Mailserver gespeicherten E-Mails durch Zugangssicherungen – etwa durch Verwendung eines Passworts – vor einem ungewollten Zugriff Dritter zu schützen. Der Provider und damit auch die Ermittlungsbehörden bleiben jedoch weiterhin in der Lage, jederzeit auf die auf dem Mailserver gespeicherten E-Mails zuzugreifen. Der Kommunikationsteilnehmer hat keine technische Möglichkeit, die Weitergabe der E-Mails durch den Provider zu verhindern. Dieser technisch bedingte Mangel an Beherrschbarkeit begründet die besondere Schutzbedürftigkeit durch das Fernmeldegeheimnis. Dies gilt unabhängig davon, ob eine E-Mail auf dem Mailserver des Providers zwischen- oder endgespeichert ist. In beiden Fällen ist der Nutzer gleichermaßen schutzbedürftig, weil sie sich hinsichtlich der faktischen Herrschaftsverhältnisse nicht unterscheiden.“[761]

In einer auf eigenständigen Kriterien basierenden, juristischen Wertung kommt es weniger auf das *technische* Ende der Übermittlung an, sondern vielmehr auf das Ende der spezifischen Gefährdungslage, für die Art. 10 I GG einen Ausgleich bietet:

„Dem Schutz der auf dem Mailserver des Providers gespeicherten E-Mails durch Art. 10 Abs. 1 GG steht nicht entgegen, dass während der Zeitspanne, während deren die E-Mails auf dem Mailserver des Providers „ruhen“, ein Telekommunikationsvorgang in einem dynamischen Sinne nicht stattfindet. Zwar definiert § 3 Nr. 22 TKG „Telekommunikation“ als den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen und bezieht sich nicht ausdrücklich auch auf statische Zustände. Art. 10 Abs. 1 GG folgt indes nicht dem rein technischen Telekommunikationsbegriff des Telekommunikationsgesetzes, sondern knüpft an den Grundrechtsträger und dessen Schutzbedürftigkeit aufgrund der Einschaltung Dritter in den Kommunikationsvorgang an.“[762]

Eine ähnliche Anknüpfung an die tatsächliche Verfügungsmacht des Betroffenen hat das BVerfG bereits in einer Entscheidung über den Zugriff auf beim Betroffenen gespeicherte Verbindungsdaten vorgenommen:

„Die Beteiligten, die ihre Kommunikation mit Hilfe von technischen Hilfsmitteln über Distanz unter Nutzung fremder Kommunikationsverbindungswege ausüben, haben nicht die Möglichkeit, die Vertraulichkeit der Kommunikation sicherzustellen.“[763]

Können die Beteiligten eigene Schutzvorkehrungen gegen einen ungewollten Datenzugriff treffen, soll diese „von dem Bürger selbst beherrschbare Privatsphäre“ laut BVerfG durch andere Grundrechte, insbesondere Art. 13 I GG und das Recht auf informationelle Selbstbestimmung, geschützt sein.[764] Sobald sich die Kommunikationsdaten in der Herrschaftssphäre des Kommunikationsteilnehmers befinden, sieht das BVerfG das Fernmeldegeheimnis nicht mehr als betroffen an:

761 BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 46.
762 BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 47.
763 BVerfG, Urteil vom 02.03.2006, Az.: 2 BvR 2099/04, Rn. 74.
764 BVerfG, Urteil vom 02.03.2006, Az.: 2 BvR 2099/04, Rn. 82; jetzt dürfte auch noch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu nennen sein.

„Der Grundrechtsschutz des Art. 10 Abs. 1 GG erstreckt sich allerdings nicht auf die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Telekommunikation, soweit dieser eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann. Dann bestehen hinsichtlich solcher Daten die spezifischen Gefahren der räumlich distanzierten Kommunikation, die durch das Telekommunikationsgeheimnis abgewehrt werden sollen, nicht fort."[765]

Maßgeblich für die Reichweite des Fernmeldegeheimnisses sind mithin die dem Einzelnen zur Verfügung stehenden *Selbstschutzoptionen*: Sind die Kommunikationsdaten den spezifischen Übermittlungsgefahren für die Vertraulichkeit der Kommunikation ausgesetzt, greift zum Ausgleich dieser Gefährdungen der rechtliche Schutz des Fernmeldegeheimnisses. Haben es dagegen die Kommunikationsteilnehmer selbst in der Hand, ihre Kommunikationsdaten auf technischem Wege zu schützen, ist der Schutzbereich des Fernmeldegeheimnisses nicht eröffnet.[766] Gelangt die durch das Fernmeldegeheimnis geschützte Kommunikation endgültig und ausschließlich in den Herrschaftsbereich des Empfängers, ist die Übermittlung nach dem BVerfG als abgeschlossen anzusehen und endet auch der grundrechtliche Schutz durch Art. 10 I GG.

(3) Inhaltliche Grenze: Sonderfall Quellen-Telekommunikationsüberwachung (Quellen-TKÜ)

Die so genannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) dient der Überwachung von Internettelefonie (auch als IP-Telefonie oder Voice-over-IP bezeichnet). Bei der Internettelefonie wird die Sprache zunächst digitalisiert. Die Audiodaten werden dann – ebenso wie bei der E-Mail-Kommunikation – in Form von Datenpaketen an den Kommunikationspartner übermittelt, basierend auf bestimmten Übertragungsprotokollen.[767] Internettelefonie kann nicht nur über den Computer erfolgen, sondern auch mittels speziell auf Internettelefonie ausgerichteter Telefone oder mit einem hergebrachten Telefon unter Verwendung eines Adapters. Eine weit verbreitete Software für Internettelefonie, „Skype", verschlüsselt die Audiodaten vor der Übermittlung standardmäßig.[768] In der technischen Übermittlungsphase können durch die Verschlüsselung weder der Netzbetreiber noch Dritte inhalt-

765 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 185 unter Bestätigung von BVerfG, Urteil vom 02.03.2006, Az.: 2 BvR 2099/04, vgl. insbes. Rn. 78.

766 Zur Frage, ob verschlüsselte Daten noch des Schutzes des Fernmeldegeheimnisses bedürfen, da sie ja als bereits technisch geschützt angesehen werden könnten, vergleiche oben unter I.1.a.bb)(3) und (4).

767 Vgl. zum technischen Hintergrund Wikipedia, IP-Telefonie, Version vom 09.06.2008, 23.32 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=IP-Telefonie&oldid=47073433 sowie *Sankol,* CR 2008, 13, 13 und *Bär,* MMR 2008, 425, 425 f.

768 Die Nutzung von „Skype" ist kostenlos und erfolgt meistens mittels zweier Computer mit entsprechendem Kopfhörer mit Mikrofon. Telefonanbieter, die reine Internettelefonie mittels regulärer Telefone (via Adapter oder mittels spezieller Endgeräte) anbieten, scheinen dagegen Übertragungsprotokolle, die die Datenpakete verschlüsseln, nicht zu unterstützen.

lich von der Kommunikation Kenntnis nehmen – auch nicht die staatlichen Sicherheitsbehörden. Daher wird im Wege der Quellen-TKÜ versucht, die Kommunikation abzuhören, indem die Audiodaten vor ihrer Verschlüsselung bzw. nach ihrer Entschlüsselung abgefangen und an die Sicherheitsbehörden weitergeleitet werden,[769] auch als „Ausleitung" bezeichnet.[770]

Dabei scheint eine ähnliche Technologie verwendet zu werden, wie sie auch zur Durchführung von Online-Durchsuchungen zum Einsatz kommen soll:[771] Zunächst muss eine Überwachungssoftware (häufig auch *`Remote Forensic Software´* genannt[772]) auf dem Zielrechner installiert werden. In der Diskussion um die Online-Durchsuchung wurden die verschiedensten Einbringungsmöglichkeiten angedacht; vom Versand von E-Mails unter dem Namen staatlicher Behörden, die im Anhang die Überwachungssoftware enthalten,[773] über die Ausnutzung von Sicherheitslücken bis zum physischen Eindringen in die Wohnung und der anschließenden manuellen Installation der Software.[774] Die Audiodatenpakete müssen via Internet an die Sicherheitsbehörden weitergeleitet werden, soweit eine Internetverbindung besteht. Anschließend soll die Software wieder vollständig vom Zielsystem entfernt werden. Damit besteht - jedenfalls in der technischen Herangehensweise – kein wesentlicher Unterschied zwischen Maßnahmen der Quellen-TKÜ und solchen zum Zweck der Online-Durchsuchung.

Zu prüfen ist daher, wie die Maßnahmen gegeneinander abgegrenzt werden können. Dies dürfte auch Auswirkungen darauf haben, welche Grundrechte jeweils als betroffen anzusehen sind.

- Unter Zugrundelegung des weiten Schutzbereichs des Fernmeldegeheimnisses fällt auch Internettelefonie unter Art. 10 I GG. Auch Daten, die in Pakete aufgeteilt via Internet versandt werden, sind vom Fernmeldebegriff umfasst. Eine Überwachung der Internettelefonie ist daher am Fernmeldegeheimnis zu mes-

769 Siehe Bundesministerium des Innern, Fragenkatalog des Bundesministeriums der Justiz, verfügbar unter: http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (31.10. 2007), S. 8 f. und 18 f.

770 *Sankol,* CR 2008, 13, 13.

771 Nach Angaben der Bundesregierung, vgl. BT-Drs 16/6885, S. 4.

772 Vgl. etwa Bundesministerium des Innern, Fragenkatalog des Bundesministeriums der Justiz, verfügbar unter: http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (31. 10.2007) 1; *Beukelmann,* StraFo 2008, 1, 1.

773 Hiervon scheint man mittlerweile abzusehen, vgl. Bundesministerium des Innern, Fragenkatalog des Bundesministeriums der Justiz, verfügbar unter: http://netzpolitik.org/wp-upload/frag en-onlinedurchsuchung-BMJ. pdf (31.10.2007), S. 14.

774 Bayern gestattete in § 34e PAG vom 01.08.2008 bis zum 31.07.2009 „das Betreten der Wohnung, die heimliche Durchsuchung der Wohnung zur Auffindung z.B. eines Notebooks und das Anbringen von Hardwarekomponenten (Z.B. von Hardware-Keyloggern zur Erfassung von Passwörtern verschlüsselter Dateien) oder das Einbringen spezifischer Software für den Zugriff auf das informationstechnische System" als so genannte Begleitmaßnahmen zur Hauptmaßnahme des verdeckten Zugriffs auf Informationssysteme; vgl. BT-Drs. 365/08, S. 14.

sen. Dabei kommt es nach Ansicht des BVerfG nicht darauf an, ob die Überwachung auf dem Übertragungsweg oder an einem Endgerät[775] erfolgt:[776]

„Der Schutzbereich dieses Grundrechts [Art. 10 I GG; d. Verf.] ist dabei unabhängig davon betroffen, ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt. Dies gilt grundsätzlich auch dann, wenn das Endgerät ein vernetztes komplexes informationstechnisches System ist, dessen Einsatz zur Telekommunikation nur eine unter mehreren Nutzungsarten darstellt."[777]

Hat die Überwachungsmaßnahme allein die *Überwachung von Internettelefonie-Kommunikation* zum Ziel, ist nach Auffassung des BVerfG einzig das *Fernmeldegeheimnis* betroffen.[778]

- Werden über die Erhebung von Inhalten und Umständen laufender Telekommunikationsvorgänge hinaus *weitere Daten* erhoben (im Wege der Durchsuchung des Systems oder durch Überwachung der Nutzung), sind diese Erhebungen nach Auffassung des BVerfG *nicht Gegenstand des Fernmeldegeheimnisses*.

  „Der durch das Telekommunikationsgeheimnis bewirkte Schutz besteht ebenfalls nicht, wenn eine staatliche Stelle die Nutzung eines informationstechnischen Systems als solche überwacht oder die Speichermedien des Systems durchsucht. Hinsichtlich der Erfassung der Inhalte oder Umstände außerhalb der laufenden Telekommunikation liegt ein Eingriff in Art. 10 Abs. 1 GG selbst dann nicht vor, wenn zur Übermittlung der erhobenen Daten an die auswertende Behörde eine Telekommunikationsverbindung genutzt wird, wie dies etwa bei einem Online-Zugriff auf gespeicherte Daten der Fall ist."[779]

  Allerdings ist eine solche Beschränkung auf Inhalte und Umstände laufender Telekommunikationsvorgänge technisch nicht abbildbar. Dringen staatliche Sicherheitsbehörden nach der oben beschriebenen Vorgehensweise in einen Rechner ein, dann ist eine Grenzziehung, welche Maßnahmen nach rechtlicher Bewertung durchgeführt werden dürfen, nicht durch technische Implementierungen umsetzbar. Nach Ansicht des BVerfG ist es bei einer Quellen-TKÜ stets möglich, weitere Daten ohne Bezug zur laufenden Telekommunikation zu erheben:

775 Vgl. auch die Legaldefinition in § 2 Nr. 6 Telekommunikations-Überwachungsverordnung (TKÜV): „Im Sinne dieser Verordnung ist […] 6. Endgerät die technische Einrichtung, mittels derer ein Nutzer einen Telekommunikationsanschluss zur Abwicklung seiner Telekommunikation nutzt […]".

776 A.A. dagegen *Sankol,* CR 2008, 13, 14 f., der nur den Übertragungsweg durch das Fernmeldegeheimnis geschützt sieht. Er verweist darauf, dass mittels der als Quellen-TKÜ bezeichneten Maßnahme kein Gespräch als Ganzes, mithin keine Kommunikation, überwacht werden könne. Erst durch das Zusammenführen der aufgezeichneten Worte ergebe sich ein Gespräch. Dies soll nach *Sankol* nicht für eine „Kommunikation" ausreichend sein.

777 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn 184.

778 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn 184. So auch *Bär,* MMR 2008, 425, 426; a.A. dagegen LG Hamburg, Beschluss vom 01.10.2007, Az.: 629 Qs 29/07, MMR 2008, 423, 424, das neben Art. 10 I GG stets auch Art. 13 I GG als betroffen ansieht, da auch das virtuelle Eindringen durch technische Mittel einen Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung darstelle.

779 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 186.

„Wird ein komplexes informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert („Quellen-Telekommunikationsüberwachung"), so ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist. Insbesondere können auch die auf dem Personalcomputer abgelegten Daten zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen. Erfasst werden können beispielsweise das Verhalten bei der Bedienung eines Personalcomputers für eigene Zwecke, die Abrufhäufigkeit bestimmter Dienste, insbesondere auch der Inhalt angelegter Dateien oder – soweit das infiltrierte informationstechnische System auch Geräte im Haushalt steuert – das Verhalten in der eigenen Wohnung."[780]

Im Wege einer Quellen-TKÜ können laut BVerfG sogar *unbeabsichtigt* weitere Daten erhoben werden. Dies wie auch das generelle Risiko unkontrollierter weiterer Datenerhebungen geht nach Ansicht des BVerfG über den Schutzbereich von Art. 10 I GG hinaus, da das Fernmeldegeheimnis derartigen Gefährdungen nicht gerecht werden kann:

„In der Folge besteht für den Betroffenen – anders als in der Regel bei der herkömmlichen netzbasierten Telekommunikationsüberwachung – stets das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden. Den dadurch bewirkten spezifischen Gefährdungen der Persönlichkeit kann durch Art. 10 Abs. 1 GG nicht oder nicht hinreichend begegnet werden."[781]

Alle Datenerhebungen durch den heimlichen Zugriff auf informationstechnische Systeme sind daher am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 I GG i.V.m. Art. 1 I GG) zu messen – wenn es sich nicht eindeutig nur um Daten bezüglich eines laufenden Telekommunikationsvorgangs via Internettelefonie handelt.[782]

- Das BVerfG begnügt sich in seiner Entscheidung zur Online-Durchsuchung aber nicht damit, nur rechtlich eine Trennung der beiden Maßnahmen Online-Durchsuchung einerseits und Quellen-TKÜ andererseits zu fordern, sondern es verlangt, dass dieses *rechtliche Trennungsgebot* auch *technisch abgebildet* wird:

„Art. 10 Abs. 1 GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer „Quellen-Telekommunikationsüberwachung", wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein."[783]

780 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 188.
781 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 189.
782 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 187: „Soweit der heimliche Zugriff auf ein informationstechnisches System dazu dient, Daten auch insoweit zu erheben, als Art. 10 Abs. 1 GG nicht vor einem Zugriff schützt, bleibt eine Schutzlücke, die durch das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Schutz der Vertraulichkeit und Integrität von informationstechnischen Systemen zu schließen ist."
783 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 190.

Es wurde bereits dargestellt, dass eine solche Trennung derzeit technisch nicht zu realisieren ist.[784] Konsequenz muss sein, dass derzeit eine *Quellen-TKÜ ausnahmsweise nicht allein am Fernmeldegeheimnis zu messen* ist, sondern *zugleich* in den *Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* (Art. 2 I GG i.V.m. Art. 1 I GG) fällt.[785] Wird in Zukunft eine saubere Trennung der Maßnahmen Quellen-TKÜ und Online-Durchsuchung technisch und rechtlich implementiert, bleibt es bei der oben dargestellten Abgrenzung: Erhebung von Inhalten und Umständen nur laufender Telekommunikation – Art. 10 I GG; Erhebung weiterer Daten – Art. 2 I GG i.V.m. Art. 1 I GG.

(4) Zusammenfassung

In seinem Geltungsbereich ist das Fernmeldegeheimnis (Art. 10 I GG) speziell und geht dem Schutz durch das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) vor, auch wenn aus beiden Gewährleistungen ein „Recht auf Verschlüsselung" deduziert werden kann.

Der Geltungsbereich des Fernmeldegeheimnisses beginnt mit dem technischen Beginn des Übermittlungsvorgangs, eine Ausdehnung oder Vorverlagerung bereits auf den Zustand der Kommunikationsbereitschaft wird vom BVerfG abgelehnt. Spiegelbildlich endet der Geltungsbereich des Fernmeldegeheimnisses mit dem Ende des Übertragungsvorgangs. Als Ende des Übertragungsvorganges in diesem Sinne ist es anzusehen, wenn die geschützte Kommunikation endgültig und ausschließlich in den Herrschaftsbereich des Empfängers gelangt. Dann ist der Betroffene durch das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG), insbesondere in seinen Ausprägungen als Recht auf informationelle Selbstbestimmung und als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, geschützt; gegebenenfalls auch durch Art. 13 I GG.

Die im Wege der Quellen-TKÜ erfolgende Überwachung von Internettelefonie ist zwar grundsätzlich analog zur herkömmlichen Telekommunikation zu behandeln. Wegen der technischen Nähe der informationstechnischen Verfahren, die zum einen für die Online-Durchsuchung und zum anderen für die Quellen-TKÜ verwendet werden, ist hinsichtlich der Quellen-TKÜ neben dem Schutzbereich des Fernmelde-

784 Daher dürften § 20l BKAG sowie der am 08.12.2009 verabschiedete neue § 15b HSOG (Art. 1, Ziffer 8 des Gesetzesentwurfs vom 30.06.2009, Drs. 18/861) derzeit ins Leere laufen: Diese fordern für eine Quellen-TKÜ, dass technisch sichergestellt wird, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird. Dies ist (derzeit) technisch nicht umsetzbar. Nach den Gesetzesbegründungen (BT-Drs. 16/9588, S. 29; Drs. 18/861, S. 14) ist die Maßnahme ansonsten bereits *unzulässig*.

785 So auch *Hornung,* CR 2008, 299, 300 f. Hornung will zudem in der bundesverfassungsgerichtlichen Forderung nach „rechtlichen Vorgaben" einen Hinweis darauf sehen, dass nach Auffassung des BVerfG die für die Quellen-TKÜ herangezogenen Ermächtigungsgrundlagen – §§ 100a, 100b StPO wie für die reguläre Telekommunikationsüberwachung auch – nicht ausreichend seien.

geheimnisses (Art. 10 I GG) auch der Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 I GG i.V.m. Art. 1 I GG) eröffnet.

bb) Unverletzlichkeit der Wohnung (Art. 13 I GG)

Des Weiteren ist das Verhältnis des Grundrechts auf Unverletzlichkeit der Wohnung (Art. 13 I GG) zum allgemeinen Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG), hier vor allem in seinen Ausprägungen als Recht auf informationelle Selbstbestimmung und als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, zu konturieren. Wie auch Art. 10 I GG enthält Art. 13 I eine spezielle Privatsphärengewährleistung. Als spezielle Norm verdrängt Art. 13 I GG in seinem Geltungsbereich daher grundsätzlich das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG).[786]

> „Mit dem Recht, in der Wohnung ungestört zu sein, und dem Recht am eigenen in der Wohnung gesprochenen Wort schützt Art. 13 Abs. 1 GG gerade den Teil der Privatsphäre, den sonst das allgemeine Persönlichkeitsrecht gewährleistet. Dieses Recht ergänzt als unbenanntes Freiheitsrecht die speziellen Freiheitsrechte, die ebenfalls konstituierende Elemente der Persönlichkeit schützen, nur insoweit, als Letztere keinen Schutz gewähren.“[787]

Im Verhältnis zum Recht auf informationelle Selbstbestimmung als Teilgehalt des allgemeinen Persönlichkeitsrechts ist Art. 13 I GG immer dann speziell, soweit es um die *Erhebung von Informationen in oder aus Wohnungen* geht.[788] Nach der Rechtsprechung des BVerfG kann im Einzelfall aber das allgemeine Persönlichkeitsrecht auch neben Art. 13 I GG anwendbar sein:

> „Art. 13 GG geht zwar als spezielleres Freiheitsrecht regelmäßig Art. 2 Abs. 1 GG vor. Das allgemeine Persönlichkeitsrecht – auch in seiner Ausprägung als Recht auf informationelle Selbstbestimmung – wird aber dort nicht verdrängt, wo sich der Schutzbereich dieses Grundrechts mit demjenigen eines speziellen Freiheitsrechts nur partiell überschneidet oder in den Fällen, in denen ein eigenständiger Freiheitsbereich mit festen Konturen erwachsen ist.“[789]

Im konkreten Fall bejahte das BVerfG diese Voraussetzungen mit der Begründung, dass sich die angegriffene Maßnahme – die Beschlagnahme eines Mobiltelefons mit dem Ziel, die auf der SIM-Karte gespeicherten Verbindungsdaten auszulesen – nicht „in der Überwindung der räumlichen Grenzen der Privatsphäre“[790] erschöpfe. Die Maßnahme wies vielmehr nach Auffassung des BVerfG eine darüber hinausweisende grundrechtliche Qualität auf. Aus dieser Begründung kann gefolgert werden, dass mit der „nur partiellen Überschneidung der Schutzbereiche“ (s.o.) Konstellationen gemeint sind, in denen eine Maßnahme in zwei (oder mehr) Grund-

786 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 73.
787 BVerfG, Urteil vom 03.03.2004, Az.: 1 BvR 2378/98 und 1084/99, Rn. 161.
788 *Hermes*, in: *Dreier,* GG, Art. 13, Rn. 119.
789 BVerfG, Urteil vom 02.03.2006, Az.: 2 BvR 2099/04, Rn. 83.
790 BVerfG, Urteil vom 02.03.2006, Az.: 2 BvR 2099/04, Rn. 84.

rechte zugleich eingreift, und dies *jeweils* mit besonderem Gewicht. Üblicherweise wird bei Informationserhebungen aus Wohnungen der Schwerpunkt in der Verletzung der räumlichen Integrität gesehen, die auch zur Erhaltung der Privatsphäre geschützt ist. Kommt den erhobenen Informationen aber besonderes Gewicht zu (hier besonderer Schutz von Telekommunikationsverbindungsdaten, die nach dem Ende der Telekommunikation nicht mehr durch Art. 10 I GG, sondern über das allgemeine Persönlichkeitsrecht geschützt sind), tritt das Recht auf informationelle Selbstbestimmung neben Art. 13 I GG. Es liegt also doch eine Überschneidung der Anwendungsbereiche vor. Diese Überschneidung ist genauso vollständig oder partiell wie in anderen Situationen von Grundrechtskonkurrenz zwischen Art. 13 I GG und Art. 2 I GG i.V.m. Art. 1 I GG auch. „Partiell" bezieht sich also darauf, dass keiner der Grundrechtseingriffe wegen seiner Qualität vollständig durch das jeweils andere Grundrecht erfasst werden kann.[791] In derartigen Konstellationen stehen mithin beide Grundrechte nach Ansicht des BVerfG nebeneinander.[792]

Eine solche Konstellation liegt auch bei einem Grundrechtseingriff durch ein absolutes Verschlüsselungsverbot vor. Ein Verschlüsselungsverbot würde vor allem gewichtig in die allgemeine Privatsphärengewährleistung durch das allgemeine Persönlichkeitsrecht (in seinen jeweiligen Teilgehalten) eingreifen. Soweit die Informationserhebung aus einer Wohnung erfolgt, ist daneben nach hier vertretener und vom BVerfG abweichender Ansicht auch Art. 13 I GG einschlägig. Die Privatsphärengefährdung, die durch ein absolutes Verschlüsselungsverbot eintreten würde, wird aber vom Recht auf Unverletzlichkeit der Wohnung nicht gänzlich erfasst. Die Privatheitsgefährdungen erreichen in einer digitalisierten Gesellschaft eine neue Qualität im Hinblick auf die Möglichkeiten umfassender Informationserhebung und –auswertung, bis hin zur Bildung von Persönlichkeitsprofilen:

> „In der Folge können sich im Arbeitsspeicher und auf den Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden. Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen."[793]

Ein derart massiver Eingriff in die Privatsphäre geht über einen Eingriff in die durch Art. 13 I GG geschützte räumliche Privatsphäre hinaus. Bei einer grundrechtlichen Bewertung eines absoluten Verschlüsselungsverbots sind daher nach hier vertretener Auffassung beide Grundrechte nebeneinander zu betrachten.

791 So auch *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 51: „Denn das `Daneben-Anwenden´ ergibt sich daraus, dass das spezielle Grundrecht den vorliegenden Lebenssachverhalt nicht voll abdeckt."

792 Für das Erheben von Daten aus Wohnung mittels einer Online-Durchsuchung hat sich für das BVerfG die Konkurrenzfrage nicht gestellt, da es – im Gegensatz zur hier vertretenen Auffassung - den Schutzbereich von Art. 13 I GG nicht als eröffnet angesehen hat (s.o.).

793 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 178.

cc) Weitere privatsphärenrelevante Grundrechte

(1) Privatsphärenrelevanz weiterer Grundrechte?

Daten, die durch das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) geschützt sind, können je nach Einzelfall – jenseits der speziellen Privatsphärengewährleistungen der Art. 10 I GG und Art. 13 I GG – auch in den Schutzbereich weiterer Grundrechte fallen, die in Teilbereichen ebenfalls einen Bezug zur Privatsphäre aufweisen.[794] Dabei wird hier zunächst erörtert, inwieweit die Schutzbereiche weiterer Grundrechte eröffnet sind.

(a) Meinungsfreiheit (Art. 5 I S. 1, 1. Hs. GG)

Private Äußerungen, in der Kommunikation mit Dritten oder in der Reflexion mit sich selbst (etwa in einem Tagebuch), enthalten zweifelsohne auch durch Art. 5 I S. 1, 1. Hs. GG geschützte Meinungen. Art. 5 I S. 1, 1. Hs. GG schützt darüber hinaus auch Tatsachenmitteilungen.[795] Letztlich gehen Meinungen und Tatsachenmitteilungen eine untrennbare Verbindung ein: Meinungen setzen Tatsachenkenntnis voraus und bilden und begründen sich auf ihrer Basis. Selbst bei vermeintlich reinen Tatsachenmitteilungen verbleibt die Auswahlentscheidung, welche Tatsachen mitgeteilt werden, als wertendes Element.[796] Grenze sind Tatsachenangaben, die keinerlei Meinungsgehalt aufweisen, wie etwa Angaben im Rahmen einer statistischen Erhebung.[797] Äußerungen im durch das allgemeine Persönlichkeitsrecht geschützten Bereich fallen daher regelmäßig auch in den Schutzbereich der Meinungsfreiheit.

Auch wenn immer wieder die grundlegende Bedeutung der Meinungsfreiheit für das demokratische Staatswesen betont wurde,[798] schützt Art. 5 I S. 1, 1. Hs. GG nicht nur die öffentliche Äußerung zur Meinungsbildung, sondern gleichermaßen die privat-individuelle Meinungsäußerung ohne politischen Bezug:[799]

> „Art. 5 I GG ist Teil des in der Menschenwürde wurzelnden elementaren Rechts auf Denkfreiheit, auf die individuell-private Befriedigung von geistiger Neugier, Wissensdurst und Mittei-

794 *Scholz/Pitschas*, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, S. 89 f.; *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 135 ff.

795 Reichweite und Grenzen der Meinungsfreiheit sind dabei in Rechtsprechung und Literatur noch nicht abschließend geklärt. Allgemein setzt sich aber ein weiter Meinungsbegriff durch. Vgl. insoweit zu den unterschiedlichen Positionen, jeweils m.w.N. *Meyn*, Verschlüsselung und Innere Sicherheit, S. 66 ff.

796 Vgl. zu allen vorgenannten Argumenten *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 5, Rn. 26; *Schulze-Fielitz*, in: *Dreier,* GG, Art. 5 I, II, Rn. 62 ff.

797 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 5, Rn. 26.

798 Vgl. etwa *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 180 ff. m.w.N.; *Dreier*, Dimensionen der Grundrechte, S. 38; *Meyn*, Verschlüsselung und Innere Sicherheit, S. 73.

799 *Schulze-Fielitz*, in: *Dreier,* GG, Art. 5 I, II, Rn. 40; *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 66; *Meyn*, Verschlüsselung und Innere Sicherheit, S. 74 f.

lungsbedürfnis und auf mitmenschliche Kommunikation in allen Lebensbereichen mit ihren sozialen Wirklichkeitskonstruktionen."[800]

Dabei umfasst die Meinungsfreiheit auch das Recht, seine Meinung verschlüsselt zu äußern.[801] Dafür spricht, dass der Grundrechtsträger frei in der Wahl der Form seiner Äußerung ist.[802] Insbesondere steht es dem Grundrechtsträger frei, Meinungen in Geheimschrift zu äußern.[803] *Meyn* betont schließlich den Gedanken, dass jede Kommunikation, jede Meinungsäußerung allein durch die Benutzung von Sprache oder eines sonstigen Mediums „codiert" sei.[804] Verschlüsselung sei also nur eine weitere Stufe von Codierung und daher vom Schutzbereich des Art. 5 I S. 1, 1. Hs. GG umfasst.[805] Weiter kann man daraus, dass die Meinungsfreiheit das Äußern und Verbreiten von Meinungen genauso wie das Nicht-Äußern und Nicht-Verbreiten einer Meinung schützt, schließen, dass Art. 5 I S. 1, 1. Hs. GG das Recht beinhaltet, den Rezipientenkreis einer Meinungsäußerung zu bestimmen.[806] Klar ist jedenfalls, dass nur deswegen, weil eine Meinung verschlüsselt und damit nicht für die Allgemeinheit geäußert wird, nicht der Äußerungscharakter entfällt. Vielmehr umfasst die Meinungsfreiheit auch ein Recht auf Verschlüsselung seiner Meinungen.

„Die Gewährleistung, seine Meinung frei zu äußern und zu verbreiten, bedeutet die Freiheit von staatlicher Lenkung, Behinderung und sonstiger Beeinträchtigung. […]; zu den faktischen Beeinträchtigungen rechnen auch das heimliche Abhören oder das heimliche Festhalten von Äußerungen durch Tonbandaufnahmen, weil hierdurch die Integrität einer Meinungsäußerung, ihre Unbefangenheit, Exklusivität oder Vertraulichkeit angetastet wird."[807]

Insbesondere im Bereich der privaten Kommunikation ist mithin neben dem Schutzbereich des allgemeinen Persönlichkeitsrechts (Art. 2 I GG i.V.m. Art. 1 I GG)[808] auch der Schutzbereich der Meinungsfreiheit (Art. 5 I S. 1, 1. Hs. GG) eröffnet.[809] Schutzbereichsüberlappungen zwischen Art. 5 I S. 1, 1. Hs. GG und Art. 2 I

800 *Schulze-Fielitz*, in: *Dreier,* GG, Art. 5 I, II, Rn. 40.

801 Vergleiche dazu ausführlich *Meyn*, Verschlüsselung und Innere Sicherheit, S. 84 ff. Auch *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 46 sympathisiert mit der Idee, ein Recht auf Verschlüsselung bei Art. 5 GG zu verorten.

802 *Schulze-Fielitz*, in: *Dreier,* GG, Art. 5 I, II, Rn. 75; *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 5, Rn. 28 ff.

803 *Schulze-Fielitz*, in: *Dreier,* GG, Art. 5 I, II, Rn. 75; *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 5, Rn. 30.

804 Siehe dazu auch das anschauliche Beispiel bei *Koops*, The crypto controversy, S. 128.

805 *Meyn*, Verschlüsselung und Innere Sicherheit, S. 84 ff., insbes. S. 91.

806 So auch *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 186.

807 *Wendt*, in: *v. Münch/Kunig,* GG, Art. 5, Rn. 18.

808 Daneben ist regelmäßig auch der Schutzbereich des Fernmeldegeheimnisses (Art. 10 I GG) eröffnet, da es sich – soweit es um ein Recht auf Verschlüsselung geht – um Datenkommunikation handelt, sei es per E-Mail oder per Internettelefonie. Insoweit wäre dann ohnehin das Fernmeldegeheimnis speziell. Gleichwohl sind natürlich Konstellationen denkbar, in denen Meinungsfreiheit und allgemeines Persönlichkeitsrecht betroffen sind, das Fernmeldegeheimnis aber nicht. Simples Beispiel wäre etwa die Nutzung des Computers wie eine Schreibmaschine zum Verfassen privater Briefe.

809 A.A. wohl *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 84, der die Zielrichtung der Meinungsfreiheit auf Beeinflussung von politischen Willensbildungsprozessen be-

GG i.V.m. Art. 1 I GG betreffen aber nur diesen Teilbereich des umfassenden Privatsphärenschutzes durch das allgemeine Persönlichkeitsrecht. Private Daten auf dem eigenen Rechner wie private Bilder, Bankdaten, Gesundheitsdaten, Steuerdaten etc. werden dagegen in der Regel nicht den Schutzbereich der Meinungsfreiheit berühren.

(b) Informationsfreiheit (Art. 5 I S. 1, 2. Hs. GG)

Die Informationsfreiheit (Art. 5 I S. 1, 2. Hs. GG) gewährleistet die Freiheit des Einzelnen, sich zu informieren. Soweit es um private Kommunikation geht, kann es zu keinerlei Schutzbereichsüberlappungen des allgemeinen Persönlichkeitsrechts mit der Informationsfreiheit kommen, da diese nur die Freiheit gewährleistet, sich aus *allgemein zugänglichen* Quellen zu informieren.[810] Eine verschlüsselte Quelle ist regelmäßig nicht allgemein zugänglich; die Verschlüsselung soll ja gerade die Kenntnisnahme durch jedermann verhindern.

Geht es aber um die Beobachtung und Registrierung von Informationsverhalten, stellt dies einen Eingriff in die Informationsfreiheit aus Art. 5 I S. 1, 2. Hs. GG dar, da dieser die *ungehinderte* Information aus allgemein zugänglichen Quellen gewährleistet. Die aus einer Beobachtung und Registrierung persönlichen Verhaltens möglicherweise resultierenden Einschüchterungseffekte[811] stellen ein Hindernis in diesem Sinne dar. [812] Soweit es darum geht, dem Einzelnen ein Recht auf anonyme Internetnutzung zu gewähren, beinhaltet somit auch die Informationsfreiheit ein Recht auf Verschlüsselung. Anonyme Internetnutzung wird nach dem derzeitigen Stand der Technik wesentlich durch den Einsatz von Verschlüsselungsverfahren verwirklicht. Unbeobachtetes Informationsverhalten wird im Wege des Rechts auf informationelle Selbstbestimmung daneben auch als Teilgehalt des allgemeinen Persönlichkeitsrechts geschützt (s.o. unter III.1.c.).

(c) Glaubens-, Bekenntnis- und Gewissenfreiheit (Art. 4 I GG)

Die Glaubens-, Bekenntnis- und Gewissenfreiheit (Art. 4 I GG) unterstellt einen weiteren Teilbereich des allgemeinen Persönlichkeitsrechts (Art. 2 I GG i.V.m. Art. 1 I GG) besonderem Schutz.[813] Art. 4 I GG schützt dabei umfassend die inneren religiösen oder weltanschaulichen Überzeugungen (forum internum), die Bildung einer Glaubensvorstellung oder Gewissenentscheidung sowie die Äußerung dieser

tont und es daher für eine Verkehrung des Sinngehalts der Kommunikationsgrundrechte hält, wenn man in diesen spezialgrundrechtlichen Privatsphärenschutz verorten würde.

810 Grundsätzlich stellt das Internet eine allgemein zugängliche Quelle dar; *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 5, Rn. 42; *Bethge*, in: *Sachs*, GG, Art. 5, Rn. 54; *Schulze-Fielitz*, in: *Dreier,* GG, Art. 5 I, II, Rn. 77.

811 Siehe zu Existenz und Grundrechtsrelevanz derartiger Einschüchterungseffekte oben A.I.3.c.dd)(4).

812 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 5, Rn. 56.

813 *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 149.

Vorstellungen und ganz allgemein die Ausrichtung seines Lebens nach den eigenen religiösen oder weltanschaulichen Überzeugungen.[814] Geschützt ist ebenso die negative Freiheit, eine bestimmte Weltanschauung oder einen bestimmten Glauben nicht zu haben und/oder nicht zu bekennen. Daten mit Bezug etwa zur Bildung von Glaubensvorstellungen oder Gewissenentscheidungen oder sonstige Daten mit religiösen oder weltanschaulichen Äußerungen werden daher auch durch Art. 4 I GG geschützt. Einfache Beispiele wären etwa tagebuchartige Aufzeichnungen in digitaler Form, die sich mit Glaubens- oder Gewissensfragen auseinandersetzen,[815] oder E-Mail-Kommunikation in diesem Themenbereich, sei es mit einem Geistlichen, sei es mit einer sonstigen Person.

> „Die negative Bekenntnisfreiheit enthält für die Behörden ein thematisch begrenztes Verbot der Informationsermittlung und –verwertung, soweit nicht der Einzelne freiwillig und gegenüber dem Staat seine Zurückhaltung aufgibt."[816]

In diesem Bereich muss es zum effektiven Schutz der Entscheidung des Grundrechtsträgers, seine Glaubens- oder Gewissensvorstellung nicht in der Öffentlichkeit zu äußern, ein Recht auf Vertraulichkeit[817] und somit auch ein Recht auf Verschlüsselung geben.

(d) Schutz von Ehe und Familie (Art. 6 I GG)

Schutzbereichsüberlappungen des allgemeinen Persönlichkeitsrechts (Art. 2 I GG i.V.m. Art. 1 I GG) finden sich auch im Verhältnis zu Art. 6 I GG als Ausdruck der „spezifischen Privatsphäre für Ehe und Familie".[818] Eheliche und familiäre Kommunikation genießt daher einen besonderen Vertraulichkeitsschutz.[819] Daraus ergibt sich mit den analogen Argumenten wie beim allgemeinen Persönlichkeitsrecht ein Recht auf Verschlüsselung.

(e) Versammlungsfreiheit (Art. 8 I GG)

Auch zwischen der Versammlungsfreiheit (Art. 8 I GG) und dem allgemeinen Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) kann es zu Überschneidungen der Schutzbereiche kommen.[820] Ebenso wie der Meinungsfreiheit kommt der Versammlungsfreiheit nicht nur demokratisch-funktionale Bedeutung zu (im Sinne der kollek-

814 *Morlok*, in: *Dreier,* GG, Art. 4, Rn. 58 ff.
815 Beispiel nach *Morlok*, in: *Dreier,* GG, Art. 4, Rn. 59.
816 *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 151.
817 Dem entspricht etwa das Zeugnisverweigerungsrecht für Geistliche in ihrer Eigenschaft als Seelsorger aus § 53 I S. 1, Nr. 1 StPO.
818 BVerfGE 6, 55, 81; *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 173.
819 *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 174.
820 Während *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 179 ff. sowohl Art. 8 I GG als auch Art. 9 I GG zu den speziellen Privatsphärengewährleistungen zählt, lehnt etwa *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 3, 41 dies ab.

tiven Meinungsäußerung zur Teilhabe an der öffentlichen Meinungsbildung[821]).[822] Art. 8 I GG schützt vielmehr zum einen *auch nicht-öffentliche Versammlungen*, zum anderen Versammlungen *zu jedem Zweck*, sei er religiös, politisch, privat etc.[823] Virtuelle Versammlungen sind allerdings nicht vom Schutzbereich erfasst:[824] Aus dem Wortlaut „sich […] versammeln" und der Entstehungsgeschichte der Norm ergibt sich, dass eine körperliche Zusammenkunft der Versammlungsteilnehmer erforderlich ist.[825] Dafür spricht, dass Versammlungen der kollektiven Meinungsbildung und –äußerung dienen sowie die innere Verbundenheit der Teilnehmer zu einem gemeinsamen Zweck erfordern. Dies setzt Kommunikationsmöglichkeiten unter den Teilnehmern voraus,[826] die bei einer virtuellen Versammlung technisch entsprechend abgebildet werden müssten.[827] Versammlungen im Internet, die unter den verfassungsrechtlichen Versammlungsbegriff des Art. 8 I GG fallen würden, sind daher derzeit nicht absehbar.

Art. 8 I GG schützt aber nicht nur die Teilnahme an, sondern auch den *Aufruf* zu und die *Organisation von Versammlungen*.[828] Dies kann natürlich auch via Internet und E-Mail erfolgen. Diese Kommunikation ist sowohl durch die Versammlungsfreiheit als auch durch das allgemeine Persönlichkeitsrecht geschützt. Zum Schutz vor Kenntnisnahme durch Dritte muss es dem Grundrechtsträger gestattet sein, seine Kommunikation zu verschlüsseln. Relevante faktische Beeinträchtigungen der Versammlungsfreiheit, die Eingriffscharakter haben können, könnten hier vor allem die Beobachtung und Registrierung von Kommunikation im Vorfeld von Versammlun-

821 *Schulze-Fielitz*, in: *Dreier,* GG, Art. 8, Rn. 27.

822 So *Dreier*, Dimensionen der Grundrechte, S. 38: „Jede Grundrechtswahrnehmung, die den Prozess politischer Willensbildung auf gesellschaftlicher wie staatlicher Ebene (mit)trägt, weist über diese Seite hinaus. Nicht um Ausgrenzung geht es dann, sondern um Mitwirkung, Gestaltung, ja in gewisser Weise um „Teilhabe" am politischen Gemeinwesen: Diese demokratiekonstitutive, der Bewahrung und Stabilisierung der freien politischen Ordnung dienliche Seite der Grundrechte liegt für die Kommunikationsgrundrechte, also in Sonderheit die Versammlungs- und Vereinigungsfreiheit, aber auch die Meinungsfreiheit auf der Hand."

823 *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 8, Rn. 17 f.; *Schulze-Fielitz*, in: *Dreier,* GG, Art. 8, Rn. 26; *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 181.

824 *Schulze-Fielitz*, in: *Dreier,* GG, Art. 8, Rn. 31; *Seidel,* DÖV 2002, 283, 285; *Kraft/Meister,* MMR 2003, 366, 366 f.; *Kraft/Meister,* K&R 2005, 458, 460 f.

825 Vgl. ausführlich zu der Frage, ob es sich um einen geographisch definierten Ort handeln muss oder nicht in teleologischer Auslegung auch die „Parallelwelt" des Internet einen Versammlungsort darstellen könnte *Kraft/ Meister,* MMR 2003, 366, 367 f. Die Autoren verneinen im Ergebnis eine Ausdehnung des Anwendungsbereichs von Art. 8 I GG.

826 *Kraft/Meister,* MMR 2003, 366, 368.

827 Dies ist bisher nicht gelungen. Bisher wurde die Frage aber – soweit ersichtlich – auch erst einmal rechtlich relevant. Das AG Frankfurt a.M. hatte über die Strafbarkeit einer so genannten „Online-Demo" zu entscheiden. Bei dieser „Online-Demo" führten die Teilnehmer eine `*Distributed Denial of Service´*-Attacke auf die Server der Lufthansa durch, um so gegen die Beteiligung der Lufthansa an der Durchführung von Abschiebungen zu protestieren; vgl. AG Frankfurt a.M., Urteil vom 01.07.2005, Az.: 991 Ds 6100 Js 226314/01, MMR 2005, 863-868.

828 *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 8, Rn. 30; *Schulze-Fielitz*, in: *Dreier,* GG, Art. 8, Rn. 32.

gen sein, die die genannten Einschüchterungseffekte und Abschreckungswirkungen haben können:[829]

> „Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten.“[830]

Vertrauliche und somit auch verschlüsselte Kommunikation muss daher insbesondere auch im Vorfeld von Versammlungen möglich sein.

(f) Vereinigungs- und Koalitionsfreiheit (Art. 9 I, III GG)

Ähnliches gilt für die Vereinigungs- (Art. 9 I GG) und die Koalitionsfreiheit (Art. 9 III GG). Auch hier muss hinsichtlich der geschützten Bildung und inneren Selbstorganisation von Vereinigungen oder Koalitionen die diesbezügliche Kommunikation der Grundrechtsträger ebenfalls vom Schutzbereich erfasst sein.[831] Dabei schützt Art. 9 GG ebenso wie Art. 8 I GG den Teilbereich der Autonomie der Selbstdarstellung des allgemeinen Persönlichkeitsrechts:[832]

> „Mit der Freiheit, den jeweiligen Kommunikationspartner zu wählen und ihm gegenüber Meinungen kundzutun, ist zugleich auch die Freiheit garantiert, seine Meinungsäußerungen dem jeweiligen Adressaten gegenüber zu dosieren, also auszuwählen, welche ´Meinung` in welchem Umfang ihm gegenüber offenbart werden soll. Somit ist die *Meinungsäußerung* nicht nur elementarer Bestandteil der Persönlichkeitsentfaltung, sondern gleichzeitig *von prägender Bedeutung für das Persönlichkeitsbild*, das der Umwelt vermittelt wird. Insoweit schützen die Kommunikationsgrundrechte zumindest für einen Teilbereich die *Autonomie der Selbstdarstellung auch in der Öffentlichkeit*. Dieser Teilbereich wird durch das Mittel der Selbstdarstellung, nämlich Meinungsäußerung, Versammeln oder Mitgliedschaft in Vereinigungen, umrissen.“[833]

Daraus folgt, dass der Einzelne berechtigt sein muss, seine insoweit grundrechtsrelevante Kommunikation gegen Kenntnisnahme durch Dritte zu sichern.

829 *Schulze-Fielitz*, in: *Dreier,* GG, Art. 8, Rn. 62; *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 8, Rn. 44; *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 186 ff.

830 BVerfGE 65, 1, 43.

831 Vergleiche zur herausragenden Bedeutung von Kommunikation für die Koalitionsfreiheit den Schriftsatz vom 11.06.2008 im Verfassungsbeschwerdeverfahren von ver.di gegen die Vorratsdatenspeicherung, http://presse.verdi.de/aktuelle-themen/vorratsdatenspeicherung/data/Verfassungsbeschwerde_Vorratsdatenspeicherung_16-06-2008.pdf (09.07.2008), insbes. S. 14 ff.

832 *Scholz/Pitschas*, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, S. 25.

833 *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 186 f.

(2) Verhältnis des allgemeinen Persönlichkeitsrechts zu partiell privatsphärenrelevanten Grundrechten

Zu untersuchen ist, wie sich das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) und die privatsphärenrelevanten Teilgewährleistungen in anderen Grundrechten (Art. 4 I GG, Art. 6 I GG, Art. 5 I S. 1 GG, Art. 8 I GG sowie Art. 9 I, III GG) zueinander verhalten:

- Für manche Konstellationen wurde das Verhältnis des allgemeinen Persönlichkeitsrechts (Art. 2 I GG i.V.m. Art. 1 I GG) zu anderen Grundrechten, die teilweise privatsphärenrelevanten Schutz entfalten können, bislang in der Rechtsprechung des BVerfG überhaupt *noch nicht erörtert* (so etwa für das Verhältnis der Informationsfreiheit zum allgemeinen Persönlichkeitsrecht im Hinblick auf anonyme Internetnutzung).
- Teilweise wurde vorgeschlagen, nicht nur die „klassischen" speziellen Privatsphärengewährleistungen der Art. 10 I GG und Art. 13 I GG als *gegenüber dem allgemeinen Persönlichkeitsrecht vorrangig* zu betrachten, sondern auch dann Spezialgrundrechten auf Konkurrenzebene den Vorrang zu lassen, wenn diese nur einen (kleinen) Teilbereich der Privatsphäre schützen (hier als partiell spezielle Privatsphärengewährleistungen bezeichnet[834]):[835]

  "Während sich die Frage des Auffangcharakters der persönlichen Entfaltungsfreiheit bei denjenigen Grundrechten nicht stellt, die keinen Bezug zur Privatsphäre haben, ergeben sich (Grundrechtskollisionen und) Grundrechtskonkurrenzen zwischen der allgemeinen Gewährleistung der Privatsphäre durch Art. 2 I/1 I GG und den Spezialgarantien der Art. 4, 6, 10 und 13 GG einerseits sowie der Art. 5, 8 und 9 GG andererseits. Dem hiesigen Verständnis der freien Entfaltung der Persönlichkeit als *Basis* eines offenen Systems grundrechtlicher Freiheitsgarantien entspricht es, den Privatsphärenschutz in erster Linie bei den einschlägigen Spezialgrundrechten zu belassen und Art. 2 I GG als Auffangposition erst dann ins Feld zu führen, wenn sie die speziellen Freiheitsrechte thematisch versagen."[836]

  Dies entspricht auch einer früher für bestimmte Konkurrenzverhältnisse vom BVerfG (etwa im Verhältnis der Meinungsfreiheit zum allgemeinen Persönlichkeitsrecht) vertretenen Auffassung.[837]

834 Von partieller Spezialität spricht auch *Scholz,* AöR 1975, 80-130, 265-290, 115; *Kahl*, Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz, S. 43 greift dies auf, verwendet aber den Terminus der Teilspezialität.

835 Dies befürwortend auch *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 237; hinsichtlich Art. 4 I GG ebenso *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 62 und wohl auch *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 3, 10. *Heß*, Grundrechtskonkurrenzen, S. 220 sieht Art. 6 I GG und Art. 4 I GG als generell spezielle Privatsphärengewährleistungen an.

836 *Scholz/Pitschas*, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, S. 89 f.

837 BVerfGE 11, 234, 238; *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 65 unter Verweis auf die vorgenannte sowie weitere Fundstellen.

- Das BVerfG tendiert in jüngerer Zeit dazu, die betroffenen Grundrechte in Verbindung miteinander anzuwenden und das eine Grundrecht als durch das oder die weitere(n) Grundrecht(e) „*ergänzt*“ oder „*verstärkt*“ [838] zu sehen:[839]

  „Die verfassungsrechtlichen Maßstäbe für die Würdigung von Äußerungen und die Zulässigkeit von Beschränkungen ergeben sich aus dem Grundrecht auf Meinungsfreiheit. Da es sich um eine Äußerung in der von Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützten Privatsphäre handelt, tritt dieses Grundrecht jedoch ergänzend hinzu.“[840]

  „Wie das Bundesverfassungsgericht entschieden hat, erfährt das durch Art. 2 Abs. 1 GG verbürgte Gebot der Achtung der Entfaltungsfreiheit im privaten Lebensbereich durch die Verfassungsgarantie von Ehe und Familie eine besondere Verstärkung.“[841]

- Eine weitere in der Literatur vertretene Auffassung[842] will die betroffenen Grundrechte schlicht *nebeneinander* prüfen im Sinne einer echten Idealkonkurrenz.[843]

(a) Genereller Vorrang auch der nur partiell speziellen Privatsphärengewährleistungen?

Eine generelle Spezialität auch der nur partiell speziellen Privatsphärengewährleistungen (Art. 4 I GG, Art. 6 I GG, Art. 5 I S. 1 GG, Art. 8 I GG sowie Art. 9 I, III GG) ist abzulehnen. Gegen die Annahme eines generellen Vorrangs der partiell speziellen Privatsphärengewährleistungen gegenüber dem allgemeinen Persönlichkeitsrecht sprechen im Wesentlichen zwei Argumente:

838 In Literatur und Rechtsprechung finden sich beide Termini, Schutzbereichsergänzung (vgl. etwa *Kahl*, Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz) und Schutzbereichsverstärkung (etwa bei *Spranger,* NJW 2002, 2074). Auch das BVerfG verwendet beide Termini und spricht teilweise – etwa in der Entscheidung zum Schächten (BVerfG, Urteil vom 15.01.2002, Az.: 1 BvR 1783/99, Rn. 32) – von „verstärken“ und teilweise – etwa in der Entscheidung zur akustischen Wohnraumüberwachung (BVerfG, Urteil vom 03.03.2004, Az.: 1 BvR 2378/98 und 1084/99, Rn. 163) – von „ergänzen“. Eine inhaltliche Abweichung scheint sich aus der unterschiedlichen Terminologie nicht zu ergeben. Hier wird der Begriff Schutzbereichsverstärkung bevorzugt, da er die Wirkung des hinzutretenden Grundrechts – Verstärkung des Schutzes des betroffenen „Haupt“grundrechts – zu konkretisieren versucht, während die Bezeichnung „Schutzbereichsergänzung“ keine inhaltliche Aussage trifft.

839 So sieht das BVerfG etwa bei Meinungsäußerungen im Bereich der Privatsphäre die Meinungsfreiheit (Art. 5 I S. 1, 1. Hs. GG) durch das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) ergänzt: BVerfGE 35, 35, 39; BVerfGE 90, 255, 259; so auch *Schulze-Fielitz*, in: *Dreier,* GG, Art. 5 I, II, Rn. 317. Das allgemeine Persönlichkeitsrecht wird nach der Rechtsprechung des BVerfG durch Art. 6 I GG zwischen Ehegatten und im Eltern-Kind-Verhältnis verstärkt: BVerfGE 57, 170, 178; ebenso *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 69; *Gröschner*, in: *Dreier,* GG, Art. 6, Rn. 155.

840 BVerfGE 90, 255, 259.

841 BVerfGE 57, 170, 178.

842 So für Art. 4 I GG *Morlok*, in: *Dreier,* GG, Art. 4, Rn. 188.

843 Siehe ausführlich zur Idealkonkurrenz *Kahl*, Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz, S. 25 ff. sowie *Heß*, Grundrechtskonkurrenzen, S. 68 ff.

Zum einen hat der Schutz der Privatsphäre mit dem Recht auf informationelle Selbstbestimmung und dem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eine derartige grundrechtliche Relevanz, Konkretisierung und spezielle Ausformung erhalten, dass der in der obigen Auffassung stets mitschwingende Gedanke des Auffangcharakters (und der Subsidiarität) von Art. 2 I GG mittlerweile als zu eindimensional erscheint. Soweit es um den Teilbereich des allgemeinen Persönlichkeitsrechts geht, ist dieser mit den Ausformungen der informationellen Selbstbestimmung und der Vertraulichkeit und Integrität informationstechnischer Systeme als in der Grundrechtssystematik vollständig gleichberechtigtes Spezialgrundrecht anzusehen – und nicht als bloßes Auffanggrundrecht.[844] In den letzten Jahren waren sowohl die allgemeine Privatsphärengewährleistung durch das allgemeine Persönlichkeitsrecht als auch die speziellen Privatsphärengewährleistungen vielfach Gegenstand verfassungsgerichtlicher Entscheidungen.[845] Vor diesem Hintergrund muss das Verhältnis partiell spezieller Privatsphärengewährleistungen und allgemeiner Privatsphärengewährleistung konturiert werden – auch nach Auffassung des BVerfG:

> „Der Gedanke des Vorrangs der Spezialnorm wird immer zutreffen, wenn die spezielle Norm nur als Ausformung der allgemeinen Norm erscheint, so daß in jener notwendig diese mit betroffen ist; anders liegt es, wenn der Sinngehalt der "besonderen" Norm zunächst von der "allgemeinen" Norm unabhängig ist, also jede eine spezifische Bedeutung hat, so daß eine Verletzung der "speziellen" Norm ohne gleichzeitige Verletzung der "allgemeinen" denkbar ist. Welche Norm als primär verletzt anzusehen ist, wird bei solcher Lage davon abhängen, welche von beiden nach ihrem spezifischen Sinngehalt die stärkere sachliche Beziehung zu dem zu prüfenden Sachverhalt hat und sich deshalb als der adäquate Maßstab erweist.“[846]

844 So auch *Hufen*, Schutz der Persönlichkeit und Recht auf informationelle Selbstbestimmung, in: *Badura/Dreier,* Festschrift 50 Jahre Bundesverfassungsgericht, S. 105, 110; *Scholz,* AöR 1975, 80-130, 265-290, 116 m.w.N.; *Rohlf,* Der grundrechtliche Schutz der Privatsphäre, S. 236; *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 49; a.A. *Kahl*, Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz, S. 58 f.

845 Etwa die Entscheidung vom 03.04.2004, Az.: 1 BvR 2378/98 und 1084/99, zur akustischen Wohnraumüberwachung; die Entscheidung vom 12.04.2005, Az.:2 BvR 1027/02, zur Beschlagnahme ganzer Datenbestände; die Entscheidung vom 12.04.2005, Az.: 2 BvR 581/01, zur GPS-Überwachung; die Entscheidung vom 27.07.2005, Az.:1 BvR 668/04, zur präventiven Telekommunikationsüberwachung; die Entscheidung vom 02.03.2006, Az.: 2 BvR 2099/04, zur Beschlagnahme eines Mobiltelefons zum Auslesen von Verbindungsdaten; die Entscheidung vom 04.04.2006, Az.: 1 BvR 518/02, zur Rasterfahndung; die Entscheidung vom 16.06.2009, Az.: 2 BvR 902/06, zur Beschlagnahme von E-Mails; die Entscheidung vom 22.08.2006, Az.: 2 BvR 1345/03, zum IMSI-Catcher; die Entscheidung vom 23.10.2006, Az.: 1 BvR 2027/02, zur versicherungsvertraglichen Obliegenheit einer Schweigepflichtentbindung; die Entscheidung vom 27.02.2008, Az.:1 BvR 370/07 und 595/07, zur Online-Durchsuchung; die Entscheidung vom 10.03.2008, Az.: 1 BvR 2388/03, zur Datensammlung über steuerrechtliche Auslandsbeziehungen; die Entscheidung vom 11.03.2008, Az.: 1 BvR 2074/05 und 1254/07 zur automatisierten Kennzeichenerfassung; die Entscheidung vom 02.03.2010, Az.: 1 BvR 256/08 et al. zur Vorratsdatenspeicherung.

846 BVerfGE 13, 290, 296.

Die erstgenannte Konstellation liegt hinsichtlich der speziellen Privatsphärengewährleistungen durch Art. 10 I GG und Art. 13 I GG vor. Daher bleibt es hier bei der Spezialität dieser Grundrechte gegenüber dem allgemeinen Persönlichkeitsrecht – mit den oben (unter aa) und bb)) dargestellten besonderen Maßgaben.

Hinsichtlich der soeben unter cc. aufgeführten Grundrechte liegt die zweite vom BVerfG genannte Konstellation vor; eine Verletzung der „speziellen" Norm ohne gleichzeitige Verletzung der „allgemeinen" Norm ist möglich – da die Spezialität eben nur in bestimmten Konstellationen vorliegt, aber nicht in allen:

- Die Meinungsfreiheit (Art. 5 I S. 1, 1. Hs. GG) schützt nicht nur private und politische Äußerungen des Einzelnen, die weitgehend als Ausdruck der ebenfalls vom allgemeinen Persönlichkeitsrecht umfassten Selbstdarstellung in der Öffentlichkeit[847] verstanden werden können, sondern auch Wirtschaftswerbung,[848] die keinen Bezug zum allgemeinen Persönlichkeitsrecht aufweist.
- Die Informationsfreiheit (Art. 5 I S. 1, 2. Hs. GG) schützt umfassend die Information aus allgemein zugänglichen Quellen, nicht nur das privatsphärenrelevante Informationsverhalten ohne Registrierung oder Beobachtung.
- Die Glaubens-, Bekenntnis- und Gewissensfreiheit (Art. 4 I GG) umfasst gerade auch das Recht des Einzelnen, sein Leben nach diesen Überzeugungen auszurichten. Handlungen, die einer religiösen oder weltanschaulichen Überzeugung geschuldet sind, fallen in den Schutzbereich von Art. 4 I GG,[849] sind aber nicht per se Gegenstand des allgemeinen Persönlichkeitsrechts.[850]
- Der Schutz von Ehe und Familie (Art. 6 I GG) gewährleistet nicht nur die eheliche oder familiäre Privatsphäre, sondern umfasst etwa bereits die (positive und negative) Eheschließungsfreiheit, die auch ein Recht auf Ehescheidung begründet.[851] Art. 6 I GG gebietet weiter eine ehe- und familiengerechte Ausgestaltung etwa des Steuerrechts.[852]
- Die Versammlungsfreiheit (Art. 8 I GG) gewährleistet in erster Linie die Teilnahme an Versammlungen und schützt damit gerade auch nicht-anonymes Verhalten in der Öffentlichkeit.[853]
- Auch die Vereinigungs- und Koalitionsfreiheit (Art. 9 I, III GG) schützt in erster Linie das Bilden von und die Tätigkeit in Vereinigungen und Koalitionen. Diese Organisationsmaßnahmen haben zumeist keinen Privatsphärenbezug.

Nach Auffassung des BVerfG müsste jeweils die „stärkere sachliche Beziehung" zum Sachverhalt im Einzelfall über die Anwendung von partieller Spezialgewähr-

847 Vgl. dazu *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 31, 42 ff.; *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 187.

848 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 5, Rn. 25.

849 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 4, Rn. 37 ff.

850 Etwa wenn es um karitative Krankenpflege, Spendensammlungen, Reisen mit religiösem oder weltanschaulichen Hintergrund, Kleidung etc. geht; Beispiele nach *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 4, Rn. 38.

851 *Robbers*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 6, Rn. 51 ff.

852 *Robbers*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 6, Rn. 104 ff.

853 *Rohlf*, Der grundrechtliche Schutz der Privatsphäre, S. 188.

leistung oder allgemeiner Gewährleistung entscheiden. Das Kriterium der jeweils stärkeren sachlichen Beziehung spricht aber gegen einen *generellen* Vorrang der partiell speziellen Privatsphärengewährleistungen.[854]

Gegen den generellen Vorrang partiell spezieller Privatsphärengewährleistungen spricht zweitens, dass unter Umständen ein und dieselbe äußere Handlung je nach Kontext in den Schutzbereich der einen oder der anderen partiell speziellen Privatsphärengewährleistung fallen würde und folglich ganz unterschiedlichen Schranken unterworfen wäre. Das hier maßgebliche Beispiel eines Rechts auf Verschlüsselung veranschaulicht dies eindrücklich: Warum sollte die verschlüsselte Kommunikation zu religiösen Themen anderen Schrankenvorbehalten unterliegen als die verschlüsselte Kommunikation innerhalb der ehelichen Privatsphäre oder die sonstige durch die Meinungsfreiheit geschützte private Kommunikation? Und dies zudem in einem Bereich, in dem bereits die Kenntnisnahme, die zur Abgrenzung ja erforderlich wäre, einen Eingriff bedeuten würde?[855] Ein genereller Vorrang der partiell speziellen Privatsphärengewährleistungen vor der allgemeinen Gewährleistung durch das allgemeine Persönlichkeitsrecht (Art. 2 I i.V.m. Art. 1 I GG) ist daher keine adäquate Lösungsoption.

(b) Schutzbereichsverstärkung?

In der neueren Rechtsprechung des BVerfG[856] geht dieses nicht mehr davon aus, dass das sachnähere Grundrecht im Wege der Spezialität weitere, ebenfalls betroffene Grundrechte verdrängt. Vielmehr sieht das BVerfG den Schutzbereich des primär betroffenen Grundrechts durch das oder die sekundär betroffenen Grundrechte „verstärkt“ oder „ergänzt“:[857]

> „Der Schutz der räumlichen Privatsphäre und des allgemeinen Persönlichkeitsrechts kann schließlich in Einzelfällen durch weitere Grundrechtsgarantien ergänzt sein. So wird das Gespräch zwischen Eheleuten in der eigenen Wohnung nicht nur von Art. 13 Abs. 1 GG, sondern zusätzlich durch Art. 6 Abs. 1 GG geschützt. Auch in Bezug auf die Kommunikation mit Berufsgeheimnisträgern können neben dem grundrechtlichen Schutz der räumlichen Privatsphäre Grundrechte in Betracht kommen, die – wie etwa Art. 4 GG im Hinblick auf das Gespräch mit

854 Siehe zu Teilspezialität und Totalspezialität auch *Kahl*, Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz, S. 40 ff.

855 Grundsätzlich ist es zwar möglich, dass ein nach außen gleiches Verhalten durch unterschiedliche Grundrechte geschützt wird, je nachdem zu welchem Zweck es erfolgt, vgl. die Beispiele bei *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 54. Dies wird jedoch dann fraglicher Abgrenzungsmaßstab, wenn gerade die inhaltliche Kenntnisnahme, also die Feststellung des Zwecks, durch die Grundrechtsgewährleistungen geschützt werden soll.

856 Siehe die Beispiele bei *Spranger,* NJW 2002, 2074, 2074 f.

857 Vgl. etwa BVerfG, Urteil vom 14.07.1999, Az.: 1 BvR 2226/94 et al., Rn. 181-183; BVerfG, Urteil vom 15.01. 2002, Az.:1 BvR 1783/99, Rn. 32; BVerfG, Beschluss vom 06.09.2004, Az.:1 BvR 1279/00, Rn. 10 (juris); BVerfG, Urteil vom 04.07.2007, Az.: 2 BvE 1/06 bis 4/06, Rn. 375; BVerfG, Beschluss vom 11.05.2007, Az.: 2 BvR 543/06, Rn. 36.

einem Geistlichen – der besonderen Schutzbedürftigkeit der Kommunizierenden Rechnung tragen.“[858]

Welches der Grundrechte das verstärkte „Haupt“grundrecht darstellt und welches Grundrecht oder welche Grundrechte dieses „Haupt“grundrecht verstärken, bestimmt sich wiederum nach dem Sachnähekriterium:[859]

„Der Schutz der räumlichen Privatsphäre und des allgemeinen Persönlichkeitsrechts kann im Einzelfall durch andere Grundrechte, wie insbesondere Art. 4 Absätze 1 und 2 sowie Art. 6 Absätze 1 und 2 GG, ergänzt sein. So kann von der Abhörmaßnahme zugleich der Schutz von Gesprächen zwischen Eheleuten in der eigenen Wohnung gemäß Art. 6 GG oder der Schutz von Gesprächen mit einem Geistlichen nach Art. 4 GG betroffen sein.“[860]

Die Figur der Schutzbereichsverstärkung hat in der Literatur zahlreiche Kritik hervorgerufen:

„Dabei bleibt völlig offen, wie diese Verstärkung erfolgt und in welcher Weise sich die Verstärkung qualitativ und quantitativ auf den dergestalt ergänzten Schutzbereich auswirkt.“[861]

Bemängelt wurde vor allem, die Schutzbereichsergänzung unterlaufe die „vom Verfassungsgeber statuierte Vielfalt schrankendivergenter Grundrechte“.[862]

„Unter dem Topos der Einheit der Verfassung droht eine potentielle Entwertung und Aushöhlung der filigran abgestuften und differenzierten Systematik der Freiheitsgrundrechte.“[863]

Allerdings verbergen sich hinter dem Begriff der Schutzbereichsverstärkung durchaus unterschiedliche Ansätze zu deren Anwendungsbereich und Wirkung.[864] Diese sind zunächst herauszuarbeiten und zu analysieren:

(aa) Modifikation des Schutzbereichs

Eine der ersten, prominentesten und am heftigsten kritisierten Entscheidungen des BVerfG zur Schutzbereichsverstärkung ist die Schächt-Entscheidung.[865] Hier sah das BVerfG das Schächten selbst nicht als Akt der Religionsausübung, mithin den Schutzbereich von Art. 4 I GG nicht als eröffnet an.[866] Das BVerfG prüfte vielmehr eine Verletzung der allgemeinen Handlungsfreiheit nach Art. 2 I GG in seiner Aus-

858 BVerfG, Urteil vom 03.03.2004, Az.: 1 BvR 2378/98 und 1084/99, Rn. 163.
859 *Kahl*, Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz, S. 13.
860 BVerfG, Beschluss vom 11.05.2007, Az.:2 BvR 543/06, Rn. 36.
861 *Spranger,* NJW 2002, 2074, 2075.
862 *Kahl*, Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz, S. 47.
863 *Kahl*, Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz, S. 45.
864 *Heß*, Grundrechtskonkurrenzen, S. 84 ff. erörtert drei Ansätze, wobei der dritte von ihm diskutierte Vorschlag eines sog. „Schrankenverbunds“ vor allem im Zusammenspiel mit einer Modifikation des Schutzbereichs zu sehen zu sein scheint. Die Kritikpunkte ähneln sich jedenfalls stark. Dementsprechend erörtert *Dreier*, in: *Dreier,* GG, Vorbemerkung, Rn. 156 diese auch gemeinsam. Dem wird hier gefolgt.
865 BVerfG, Urteil vom 15.01.2002, Az.:1 BvR 1783/99 – Schächten.
866 BVerfG, Urteil vom 15.01.2002, Az.:1 BvR 1783/99, Rn. 32.

prägung als wirtschaftliche Betätigungsfreiheit[867] (und als personelles Auffangrecht, da sich der Beschwerdeführer als Ausländer nicht auf Art. 12 I GG berufen konnte). Diesen Schutzbereich sah das BVerfG dann aber wegen des dadurch erfolgenden „Ausdrucks einer religiösen Grundhaltung“[868] als durch die Religionsfreiheit verstärkt an:

> „Dem ist, auch wenn das Schächten selbst nicht als Akt der Religionsausübung verstanden wird, dadurch Rechnung zu tragen, dass der Schutz der Berufsfreiheit des Beschwerdeführers aus Art. 2 Abs. 1 GG durch den speziellen Freiheitsgehalt des Grundrechts der Religionsfreiheit aus Art. 4 Abs. 1 und 2 GG verstärkt wird.“[869]

In der Schächt-Entscheidung standen sich die Berufsfreiheit des muslimischen Metzgers und der Tierschutz gegenüber. Erst dadurch, dass es sich laut BVerfG[870] um einen „religiös geprägten Beruf“ sowie „religiös motivierte Speisevorschriften“ handelt, wird die Ausnahme von dem tierschutzgesetzlichen Gebot, warmblütige Tiere nur unter Betäubung zu töten, gerechtfertigt.[871]

Die Schächt-Entscheidung scheint ein Beispiel für eine tatsächliche *Modifikation* des Schutzbereiches zu sein, indem das BVerfG als neuartiges Schutzgut den „religiös motivierten Beruf“ kreiert und dies als das „Grundrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 4 Abs. 1 und 2 GG“[872] bezeichnet.

Zutreffend wurde diese Konstruktion als dogmatisch vollkommen unklar kritisiert.[873] Die Grenzen der Schutzbereiche der einzelnen Freiheitsrechte werden aufgehoben.[874] Gerade bei der Schächt-Entscheidung liegt der Verdacht nahe, dass rein ergebnisorientierte Erwägungen das BVerfG zu dieser dogmatischen Konstruktion veranlasst haben[875] und es zur Figur der Schutzbereichsverstärkung greift,

867 Vgl. zur wirtschaftlichen Betätigungsfreiheit *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 147.

868 BVerfG, Urteil vom 15.01.2002, Az.:1 BvR 1783/99, Rn. 32.

869 BVerfG, Urteil vom 15.01.2002, Az.:1 BvR 1783/99, Rn. 32.

870 BVerfG, Urteil vom 15.01.2002, Az.: 1 BvR 1783/99, Rn. 49.

871 Vgl. BVerfG, Urteil vom 15.01.2002, Az.: 1 BvR 1783/99, Rn. 49: „Unter diesen Umständen kann eine Ausnahme von der Verpflichtung, warmblütige Tiere vor dem Ausbluten zu betäuben, auch dann nicht ausgeschlossen werden, wenn es darum geht, einerseits die grundrechtlich geschützte Ausübung eines religiös geprägten Berufs und andererseits die Einhaltung religiös motivierter Speisevorschriften durch die Kunden des Berufsausübenden zu ermöglichen. Ohne eine derartige Ausnahme würden die Grundrechte derjenigen, die betäubungslose Schlachtungen berufsmäßig vornehmen wollen, unzumutbar beschränkt, und den Belangen des Tierschutzes wäre ohne zureichende verfassungsrechtliche Rechtfertigung einseitig der Vorrang eingeräumt. Notwendig ist stattdessen eine Regelung, die in ausgewogener Weise sowohl den betroffenen Grundrechten als auch den Zielen des ethischen Tierschutzes Rechnung trägt.“

872 BVerfG, Urteil vom 15.01.2002, Az.: 1 BvR 1783/99, Rn. 53 und 54.

873 So auch sehr kritisch *Volkmann,* DVBl. 2002, 332, 333.

874 *Spranger,* NJW 2002, 2074, 2075.

875 Siehe etwa die oben wörtlich zitierte Randnummer 49 des Urteils.

„ […] wenn das Gericht thematisch zu einem Spezialrecht tendierende Freiheiten (noch) nicht in dessen Tatbestand aufnahmen, diese aber dennoch – in Verbindung mit diesem Spezialrecht – grundrechtlich schützen will.“[876]

So hat das BVerfG in der Schächt-Entscheidung die Eröffnung des Schutzbereichs explizit verneint, um dann doch „die Besonderheiten [des abgelehnten Grundrechts; d. Verf.] zu berücksichtigen“.[877] Darin wird zum Teil eine unzulässige Schrankenleihe[878] gesehen.[879] Dogmatisch kann ein solches Vorgehen jedenfalls nicht überzeugen:

„Insgesamt besteht also die Gefahr, dass – dem Willen des Verfassungsgebers zuwider – klar definierte Grundrechtsverbürgungen zu Gunsten der Möglichkeit einer denkbar kreativen Grundrechtskonstruktion aufgegeben und so letztlich inhaltlich vollkommen neu gestaltet werden.“[880]

Das BVerfG entscheidet dabei zunehmend gar nicht mehr eindeutig darüber, ob ein Eingriff in den Schutzbereich eines Grundrechts vorliegt oder nicht.[881] Das praktische Bedürfnis nach einer Schutzbereichsmodifikation bleibt dabei teilweise im Dunkeln.[882] Eine Modifikation des Schutzbereichs ist daher abzulehnen. Eine solche

876 *Scholz,* AöR 1975, 80-130, 265-290, 119 für die Schutzbereichsergänzungsfunktion des Art. 2 I GG als Generalfreiheitsrecht.

877 BVerfG, Urteil vom 12.04.2005, Az.:2 BvR 1027/02, Rn. 90: „Die angegriffenen Entscheidungen greifen zwar nicht in das Grundrecht der Berufsfreiheit (Art. 12 GG) der Beschwerdeführer ein. Die Besonderheiten der beruflichen Tätigkeit der Beschwerdeführer als Rechtsanwälte und Steuerberater sind aber bei der verfassungsrechtlichen Prüfung der angegriffenen Maßnahmen zu berücksichtigen.“

878 Die Unzulässigkeit wird von *Kahl*, Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz, S. 45 als „beinahe communis opinio“ bezeichnet.

879 *Faller,* KritJ 2002, 227, 232.

880 *Spranger,* NJW 2002, 2074, 2075. So auch *Heß*, Grundrechtskonkurrenzen, S. 85, der eine solche Modifikation des Schutzbereiches unter dem Stichwort Kombinationsgrundrechte diskutiert.

881 Vgl. etwa die Entscheidung des BVerfG zur Veröffentlichungspflicht für Nebeneinkünfte von Abgeordneten, in der das BVerfG auch die Berufsfreiheit und das Recht auf informationelle Selbstbestimmung „berührt“ sah: „Nicht nur die Freiheit des Mandats wird durch diese Regulierung eingeschränkt; berührt wird auch die im Rahmen von Art. 38 Abs. 1 Satz 2 GG in dieser Konstellation ergänzend heranzuziehende grundrechtliche Rechtsstellung des Abgeordneten, insbesondere die Freiheit des Berufs und das Grundrecht auf informationelle Selbstbestimmung.“ (BVerfG, Urteil vom 04.07.2007, Az.: 2 BvE 1/06 bis 4/06, Rn. 375) oder die Entscheidung vom 06.09.2004, Az.:1 BvR 1279/00, in der das BVerfG das Persönlichkeitsrecht durch die Rundfunkfreiheit ergänzt sah: „Art. 5 Abs. 1 Satz 2 GG ist aber ergänzend heranzuziehen, soweit es um die Beurteilung von Besonderheiten einer Berichterstattung durch Rundfunk geht, und zwar insbesondere hinsichtlich der Art der medialen Darstellung und der durch die Sendung ausgelösten Wirkungen.“ (ebenda, Rn. 10 (juris)).

882 So hat das BVerfG in seinem Urteil vom 14.07.1999, Az.: 1 BvR 2226/94 et al., das Fernmeldegeheimnis durch die Pressefreiheit ergänzt gesehen: „Der auf die prinzipielle Geheimnisqualität der Kommunikation bezogene Schutz des Art. 10 GG kann schließlich durch weitere Grundrechtsgarantien ergänzt werden […] Soweit sich die Beschwerdeführer im Pressewesen betätigen und geltend gemacht haben, in dieser Tätigkeit durch die angegriffenen Vorschriften behindert zu werden, kommt dafür die Pressefreiheit aus Art. 5 Abs. 1 Satz 2 GG in

ist vorliegend auch gar nicht erforderlich, da die Schutzbereiche von allgemeinem Persönlichkeitsrecht *und* partiell speziellen Privatsphärengewährleistungen eröffnet sind, für eine Einbeziehungen von Aspekten eines Grundrechts in den Schutzbereich eines anderen also gar kein Bedürfnis besteht.

(bb) Berücksichtigung auf Verhältnismäßigkeitsebene

Dieses auch als „Begrenzungskombination“[883] bezeichnete Modell berücksichtigt die Betroffenheit mehrerer Grundrechte im Rahmen der Verhältnismäßigkeitsprüfung. Die Mehrheit der verfassungsgerichtlichen Entscheidungen zur Schutzbereichsverstärkung scheint von einem derartigen Verständnis auszugehen. So etwa die Briefkontroll-Entscheidungen des BVerfG, in denen es jeweils um ehrverletzende Äußerungen im Briefverkehr zwischen Straf- bzw. Untersuchungsgefangenen und ihren Familienangehörigen bzw. Ehepartnern ging.[884] Das BVerfG sieht diese Meinungsäußerungen in der Privatsphäre als durch Art. 5 I S. 1, 1. Hs. GG, verstärkt durch das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG), geschützt an.[885]

> „Die verfassungsrechtlichen Maßstäbe für die Würdigung von Äußerungen und die Zulässigkeit von Beschränkungen ergeben sich aus dem Grundrecht auf Meinungsfreiheit. Da es sich um eine Äußerung in der von Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützten Privatsphäre handelt, tritt dieses Grundrecht jedoch ergänzend hinzu.“[886]

Auch wenn damit auf Schutzbereichsebene ebenfalls ein neues Recht geschaffen zu werden scheint, nämlich das Recht auf Meinungsäußerungen in der Privatsphäre, wirkt sich dies hier nicht auf Schutzbereichsebene, sondern allein bei der Abwägungsentscheidung zwischen Meinungsfreiheit einerseits und Ehrschutz andererseits aus:[887]

Betracht.“ (ebenda, Rn. 181 f.). Weshalb das BVerfG keinen Eingriff in die Pressefreiheit selbst prüft, bleibt unklar.

883 So *Heß*, Grundrechtskonkurrenzen, S. 86 ff. *Dreier*, in: *Dreier,* GG, Vorbemerkung, Rn. 156 bezeichnet diese Terminologie als unglücklich, da systematisch eine Verstärkung der Schranken-Schranken vorliege. Die Terminologie von *Heß* wird daher hier auch nicht übernommen, sondern es bleibt beim vom BVerfG verwendeten Begriff der Schutzbereichsverstärkung.

884 BVerfGE 35, 35; 42, 234; 57, 170; 90, 255; Beispiele nach *Kahl*, Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz, S. 10.

885 BVerfGE 35, 35, 39; 42, 234, 236; 90, 255, 259. Ausnahme blieb die Entscheidung in BVerfGE 57, 170 ff., in der das BVerfG Art. 2 I GG durch Art. 6 I GG verstärkt sah (BVerfGE 57, 170, 178), was in der Sache aber zum selben Ergebnis führte.

886 BVerfGE 90, 255, 259.

887 A.A. *Kahl*, Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz, S. 15, der die Wirkung der Schutzergänzungsfunktion vor allem auf der Schutzbereichsebene sieht und nur ausnahmsweise auf der Ebene der verfassungsrechtlichen Rechtfertigung. Wie sich diese Wirkung auf Schutzbereichsebene darstellt, bleibt aber unklar, zumal er dann im Anschluss bei der von ihm so bezeichneten objektiven Schutzergänzung davon spricht, dass das verstärkende Grundrecht „im Rahmen der Güterabwägung mit kollidierenden Belangen als objektive

„Diese Abwägungsregel gilt aber nicht ausnahmslos. Sie beruht auf der unausgesprochenen Voraussetzung, daß die kränkende Äußerung gegenüber dem Betroffenen oder Dritten getan wird und dort ihre herabsetzende Wirkung entfaltet. An dieser Voraussetzung fehlt es, wenn die Äußerung in einer Sphäre fällt, die gegen Wahrnehmung durch den Betroffenen oder Dritte gerade abgeschirmt ist. Eine solche Sphäre wird durch das allgemeine Persönlichkeitsrecht begründet."[888]

Die Schutzbereichsverstärkung kommt danach immer dann in Betracht, wenn – wie im Falle eines Rechts auf Verschlüsselung – ein komplexer Sachverhalt gerade nicht von nur einem Spezialgrundrecht abgedeckt wird:

„Die Supplementierungswirkung kommt ferner in Betracht, wenn ein zwar nicht teilbarer, aber *vielschichtig-komplexer* Lebenssachverhalt von einem speziellen Freiheitsgrundrecht nur *partiell* abgedeckt wird."[889]

Für eine Berücksichtigung der Betroffenheit weiterer privatsphärenrelevanter Grundrechte bei der Verhältnismäßigkeitsprüfung spricht, dass nur auf diese Weise die Kumulation der Grundrechtseingriffe abgebildet werden kann. Andernfalls wären die einzelnen betroffenen Grundrechte schlicht nebeneinander zu prüfen. Für jedes betroffene Grundrecht wäre gesondert nach der verfassungsrechtlichen Rechtfertigung und insbesondere der Verhältnismäßigkeit des Eingriffs zu fragen. Insoweit beantwortet sich die Frage nach der Sinnigkeit und der Notwendigkeit einer Schutzbereichsverstärkung danach, ob man der Tatsache der kumulativen Betroffenheit mehrerer Grundrechte Bedeutung zumessen möchte oder nicht:

So wird teilweise in der Literatur vertreten, eine kumulative Betroffenheit mehrerer Grundrechte sei lediglich eine gewöhnliche grundrechtliche Konkurrenzsituation.[890] Eine Verstärkung des Schutzes komme nicht Betracht, da andernfalls nur quantitativ genügend Grundrechte betroffen sein müssten, um qualitativ den größtmöglichen Schutz zu erreichen:

„Nimmt man diese Ansicht ernst, wäre eine bis zur maximalen Verstärkung führende Kettenreaktion die Folge. Jedes weitere hinzutretende Grundrecht müßte den Qualifikationseffekt noch verstärken, so daß letztendlich der unter Verwendung künstlerischer Formensprache demonstrierende, parteilich organisierte Sekten-Guru einer der verfassungsrechtlich am besten abgesicherten Grundrechtsträger wäre."[891]

Diese Konsequenz tritt aber nur ein, wenn einerseits dem Kriterium der Betroffenheit mehrerer Grundrechte innerhalb der Abwägungsentscheidung eine gegenüber anderen Abwägungsparametern herausgehobene (und keine gleichgeordnete) Bedeutung eingeräumt würde und andererseits die Verstärkungswirkung schematisch und gleichsam rechnerisch erfolgen würde (etwa im Sinne von: zwei betroffene Grundrechte gewährleisten dann auch verdoppelten Schutz). Ein solches Vorgehen wäre abzulehnen.

Direktive einem anderen Grundrecht besonderes Gewicht" verleihe, *Kahl*, Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz, S. 16.

888 BVerfGE 90, 255, 259 f.

889 *Kahl*, Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz, S. 12.

890 *Heß*, Grundrechtskonkurrenzen, S. 88.

891 *Heß*, Grundrechtskonkurrenzen, S. 87 f.

Allerdings spricht nichts dagegen, im Rahmen der Verhältnismäßigkeit im engeren Sinne die Betroffenheit weiterer Grundrechte im Sinne einer besondere Schwere des Eingriffs zu berücksichtigen[892] – so wie auch andere qualitative und quantitative Argumente dort Berücksichtigung finden (etwa die große Streubreite einer Maßnahme, die nichts anderes als der quantitative Gesichtspunkt einer besonders hohen Zahl an Betroffen ist, oder die Verdachtslosigkeit einer Maßnahme[893] als qualitativer Gesichtspunkt für die Annahme einer besonderen Schwere des Eingriffs). Dies scheint letztlich auch von den Kritikern der Schutzbereichsverstärkung so gesehen zu werden, die sich zwar gegen ein schematisches Zusammenzählen wenden, aber durchaus für eine „Verfestigung der Basis der grundrechtlichen Abwehrrechte“[894] bei kumulativer Betroffenheit mehrerer Grundrechte eintreten, die allerdings nicht über den Schutz hinausreichen können soll, den das stärkste betroffene Grundrecht zu vermitteln imstande ist:

> „Grundrechtskombination im Sinne einer Beeinflussung der Normgehalte kann demnach nur heißen, daß ein Grundrecht – oder möglicherweise alle beteiligten Grundrechte – durch die jeweils mitbetroffenen Grundrechte eine Schutzverstärkung erfahren, die aber durch das Maß des „stärksten“ Grundrechts beschränkt ist.“[895]

Der Annahme einer besonderen Schwere des Eingriffs im Rahmen der Verhältnismäßigkeitsprüfung bei kumulativer Betroffenheit mehrerer Grundrechte stehen folglich bei Beachtung der soeben genannten Grundsätze keine dogmatischen Bedenken entgegen. Es handel sich um eine äußerst praktikable Lösung für das Problem der Grundrechtskumulation.[896]

Nach hier vertretener Auffassung ist – jedenfalls für das im Rahmen dieser Arbeit diskutierte Recht auf Verschlüsselung – das kumulative Zusammentreffen mehrerer Grundrechtseingriffe adäquat zu berücksichtigen. Ein reines Nebeneinanderprüfen der einzelnen Grundrechtseingriffe wird der tatsächlichen Situation nicht gerecht. Zwar ist es durchaus typisch, dass ein Verhalten in den Schutzbereich mehrerer Grundrechte fällt und sich so Fragen der Grundrechtskonkurrenz stellen. Die Betroffenheit eines ganzen Grundrechts*bündels* ist aber *atypisch* und muss bei der Frage der Rechtfertigung der Grundrechtseingriff berücksichtigt werden – mit den oben genannten Maßgaben.

Die Eröffnung der Schutzbereiche eines ganzen Bündels an Grundrechten spiegelt dabei den Umstand wider, dass das herausgearbeitete Recht auf Verschlüsselung den neuartigen Gefährdungen der Persönlichkeit „im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse“[897] geschuldet ist. Die zu Grunde liegenden Phänomene der zunehmenden Digitalisierung und Vernetzung, die die Erstellung umfassender Persönlichkeitsprofile sowie die Ausforschung und

892 Dazu tendieren auch Kritiker der BVerfG-Rechtsprechung in der Schächt-Entscheidung; vgl. *Faller,* KritJ 2002, 227, 228 und *Wittreck,* Der Staat 2003, 519, 523.
893 So BVerfG, Beschluss vom 04.04.2006. Az.: 1 BvR 518/02, Rn. 118 ff. – Rasterfahndung.
894 *Heß*, Grundrechtskonkurrenzen, S. 88.
895 *Heß*, Grundrechtskonkurrenzen, S. 88.
896 So auch *Heß*, Grundrechtskonkurrenzen, S. 87.
897 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 169.

Überwachung des Einzelnen in bislang unbekannter Intensität ermöglichen, wirken sich in (beinahe) allen Lebensbereichen aus. Dementsprechend sind auch nahezu alle grundrechtlichen Gewährleistungen betroffen. Dieser Betroffenheit beinahe aller Lebensbereiche und Grundrechtsgewährleistungen kann nicht durch ein schlichtes Nebeneinanderprüfen der einzelnen betroffenen Grundrechte Rechnung getragen werden. Denn wesentliche Merkmal ist gerade die *Allumfassendheit* der Digitalisierung und Vernetzung und damit der Profilbildungs- und Überwachungsmöglichkeiten. *Die besonderen Bedrohungen für die Privatsphäre des einzelnen resultieren daraus, dass Daten aus den verschiedenen Lebens- und grundrechtlichen Schutzbereichen verknüpft werden können*. Bei einem Recht auf Verschlüsselung im Rahmen des allgemeinen Persönlichkeitsrechts (Art. 2 I GG i.V.m. Art. 1 I GG) geht es gerade um den Schutz vor *umfassender* Beobachtung und Registrierung und den daraus resultierenden Einschüchterungseffekten. Insoweit ist die *Summe* der Eingriffe in die Schutzbereiche mehrerer privatsphärenrelevanter Grundrechte *mehr* als die einzelnen zu Grunde liegenden Grundrechtseingriffe.

Dieses neuartige Gefährdungspotential für die durch das allgemeine Persönlichkeitsrecht geschützte Privatsphäre rechtfertigt und erfordert die Schutzbereichsverstärkung durch die genannten partiell speziellen Privatsphärengewährleistungen. Hierin liegt auch der Grund, weswegen hinsichtlich des Fernmeldegeheimnisses (Art. 10 I GG) und des Grundrechts auf Unverletzlichkeit der Wohnung (Art. 13 I GG) eine Schutzbereichsverstärkung nicht diskutiert wurde: Die Gefährdungen für die Vertraulichkeit der räumlich distanzierten Kommunikation und die räumliche Privatsphäre haben sich zwar technisch, aber nicht wesentlich inhaltlich verändert: Das Fernmeldegeheimnis hat schon immer die Vertraulichkeit aller Arten von Kommunikation geschützt, familiäre wie religiöse Kommunikation, die Äußerung von Meinungen etc. Die räumliche Privatsphäre des Art. 13 I GG hat auch schon immer alles Verhalten innerhalb dieses Bereichs geschützt, das Familienleben wie die Religionsausübung, die Äußerung von Meinungen usw. Mit der Digitalisierung und Vernetzung haben sich insofern die technischen Möglichkeiten des Abhörens, Ausspähens und Überwachens verändert, die dahinter stehenden Bedrohungen für die Privatsphäre aber nicht. Der Schutz vor Profilbildung und Datenverknüpfung ist allein Gegenstand des allgemeinen Persönlichkeitsrechts und hier ist das neuartige Gefährdungspotential für die Privatsphäre zu verorten, welches eine Schutzbereichsverstärkung durch die ebenfalls betroffenen partiell speziellen Privatsphärengewährleistungen erforderlich macht.

Daher ist eine Schutzbereichsverstärkung des allgemeinen Persönlichkeitsrechts (Art. 2 I GG i.V.m. Art. 1 I GG) durch die partiell speziellen Privatsphärengewährleistungen der Meinungsfreiheit (Art. 5 I S. 1, 1. Hs. GG), Informationsfreiheit (Art. 5 I S. 1, 2. Hs. GG), Glaubens-, Bekenntnis- und Gewissensfreiheit (Art. 4 I GG), Versammlungsfreiheit (Art. 8 I GG), Vereinigungs- und Koalitionsfreiheit (Art. 9 I, III GG) sowie des Schutzes von Ehe und Familie (Art. 6 I GG) anzunehmen. Diese wirkt sich bei der Abwägungsentscheidung im Rahmen der Verhältnismäßigkeit im engeren Sinne aus, so dass von einer besonderen Schwere des Eingriffs auszugehen ist.

dd) Zusammenfassung

Im Verhältnis zu Art. 10 I GG und Art. 13 I GG ist das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) subsidiär, soweit deren Geltungsbereich eröffnet ist. Dabei wird der Geltungsbereich des Fernmeldegeheimnisses (Art. 10 I GG) maßgeblich durch den technischen Übermittlungsvorgang bestimmt; mit dem technischen Beginn des Übermittlungsvorgangs beginnt der Schutz des Fernmeldegeheimnisses, mit dessen technischem Ende endet auch der Grundrechtsschutz durch Art. 10 I GG. Für die Überwachung von Internettelefonie gilt grundsätzlich nichts anderes. Auf Grund technischer Besonderheiten ist aber nach derzeitigem Stand der Technik das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme neben dem Fernmeldegeheimnis anzuwenden und nicht subsidiär zu diesem.

Befinden sich Daten endgültig und ausschließlich im Herrschaftsbereich des Grundrechtsberechtigten, ist der Geltungsbereich des Fernmeldegeheimnisses nicht (mehr) betroffen, auch wenn die Daten via Telekommunikation in diesen Herrschaftsbereich gelangt sind. Diese Daten sind vielmehr durch das allgemeine Persönlichkeitsrecht geschützt. Die Daten befinden sich regelmäßig auch in der räumlich geschützten Privatsphäre des Art. 13 I GG. Da weder Art. 13 I GG noch Art. 2 I GG i.V.m. Art. 1 I GG die aus einem Verschlüsselungsverbot resultierenden Privatheitsgefährdungen gänzlich erfassen (siehe oben unter bb)), sind das allgemeine Persönlichkeitsrecht und das Recht auf Unverletzlichkeit der Wohnung insoweit nebeneinander anwendbar.

Soweit nach diesen Grundsätzen das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) anwendbar ist, findet eine Schutzbereichsverstärkung durch die Meinungsfreiheit (Art. 5 I S. 1, 1. Hs. GG), die Informationsfreiheit (Art. 5 I S. 1, 2. Hs. GG), die Glaubens-, Bekenntnis- und Gewissensfreiheit (Art. 4 I GG), die Versammlungsfreiheit (Art. 8 I GG), die Vereinigungs- und Koalitionsfreiheit (Art. 9 I, III GG) sowie den Schutz von Ehe und Familie (Art. 6 I GG) statt – wenn die Schutzbereiche dieser Grundrechte im Einzelfall eröffnet sind.

2. Grundrechtseingriff durch ein absolutes Verschlüsselungsverbot

Ein Gesetz mit einem absoluten Verbot von Verschlüsselungsverfahren würde einen Eingriff in das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) darstellen.

3. Verfassungsrechtliche Rechtfertigung eines absoluten Verschlüsselungsverbots

Ein absolutes Verschlüsselungsverbotsgesetz könnte aber verfassungsrechtlich gerechtfertigt sein.

a. Gesetzesvorbehalt

Das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) unterliegt den Schranken des Art. 2 I GG: der Rechte anderer, der verfassungsmäßigen Ordnung und des Sittengesetzes. Da die verfassungsmäßige Ordnung die Gesamtheit der Normen umfasst, die formell und materiell mit der Verfassung in Einklang stehen,[898] handelt es sich de facto um einen allgemeinen Rechtsvorbehalt.[899] Die „verfassungsmäßige Ordnung" wird als Schrankenbestimmung des allgemeinen Persönlichkeitsrechts jedoch restriktiver ausgelegt als dies im Rahmen der allgemeinen Handlungsfreiheit der Fall ist. Daher ist regelmäßig ein formelles Gesetz erforderlich;[900] wobei teilweise in der Literatur ein Gesetz im materiellen Sinne mit hohem Bestimmtheitsgrad als ausreichend erachtet wird.[901]

b. Verstoß gegen die Wesensgehaltsgarantie (Art. 19 II GG)

Ein absolutes Verschlüsselungsverbotsgesetz könnte auch den Wesensgehalt des allgemeinen Persönlichkeitsrechts, insbesondere seiner Teilgehalte des Rechts auf informationelle Selbstbestimmung und des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, antasten. Dafür sprechen sowohl eine qualitative als auch eine quantitative Betrachtungsweise des Wesensgehalts – wie auch schon im Rahmen des Fernmeldegeheimnisses:

- In einer *quantitativen Perspektive* würde allen Grundrechtsberechtigten die informationelle Selbstbestimmung im Sinne einer freiwilligen Entscheidung über die Preisgabe von personenbezogenen Daten genommen, da Daten nicht technisch gegen die Kenntnisnahme Dritter gesichert werden könnten. Der vorhandene rechtliche Schutz kann für diesen Mangel an technischer Sicherheit keinen adäquaten Ersatz bieten. Gleiches gilt für die Vertraulichkeit und Integrität von Daten ohne Personenbezug in informationstechnischen Systemen. Eine technische Kontrolle über Daten im Sinne von Vertraulichkeit, Verfügbarkeit und Anonymität wäre allen Grundrechtsberechtigten unmöglich. Dies wäre eine „vollständige Entleerung und faktische Auslöschung" [902] des allgemeinen Persönlichkeitsrecht, insbesondere seiner Teilgehalte des Rechts auf informationelle Selbstbestimmung wie des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[903]

898 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 25; *Dreier*, in: *Dreier,* GG, Art. 2 I, Rn. 54.
899 *Dreier*, in: *Dreier,* GG, Art. 2 I, Rn. 54.
900 *Dreier*, in: *Dreier,* GG, Art. 2 I, Rn. 86 m.w.N.; *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 103; *Kloepfer,* Informationsrecht, § 3, Rn. 46.
901 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 23.
902 Siehe *Dreier*, in: *Dreier,* GG, Art. 19 II, Rn. 7 sowie oben unter I.3.b.bb)(2).
903 Hier wird auf das allgemeine Persönlichkeitsrecht in allen seinen Teilgehalten verwiesen, da auch das digitalisierte eigene Bild betroffen sein könnte oder das digitalisierte Wort etc.

- In einer *qualitativen Perspektive* wären auch Daten, die zum unantastbaren Kernbereich privater Lebensgestaltung und damit zum Menschenwürdegehalt des Rechts auf informationelle Selbstbestimmung und des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gehören, von einem absoluten Verschlüsselungsverbotsgesetz betroffen. Da die zum unantastbaren Kernbereich gehörenden Daten im Hinblick auf die Internationalität der Bedrohungen und den damit einhergehenden Rechtsdurchsetzungsdefiziten weder prozedural noch – bei Erlass eines absoluten Verschlüsselungsverbotsgesetzes – technisch geschützt werden könnten, begründet auch dies einen Verstoß gegen die Wesensgehaltsgarantie.

c. Verhältnismäßigkeitsgrundsatz

Auch wenn mit der hier vertretenen Auffassung der Antastung des Wesensgehalts (Art. 19 II GG) ein Verstoß gegen das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) bereits feststeht, soll noch kurz ergänzend auf die Anforderungen des Verhältnismäßigkeitsgrundsatzes eingegangen werden: Ein absolutes Verschlüsselungsverbotsgesetz müsste des Weiteren dem Verhältnismäßigkeitsgrundsatz genügen, also einem legitimes Zweck dienen, zur Zweckerreichung geeignet und erforderlich sowie insgesamt verhältnismäßig im engeren Sinne sein.

aa) Legitimer Zweck

Ein absolutes Verschlüsselungsverbotsgesetz dient der Repression sowie der Prävention von Straftaten. Durch Verbrechensbekämpfung und Strafverfolgung wird auch der Rechtsfrieden gesichert, worin ein schützenswertes Allgemeinwohlinteresse mit eigenständigem Gewicht zu sehen ist. Dabei handelt es sich um legitime Zwecke.

bb) Geeignetheit

Ein absolutes Verschlüsselungsverbotsgesetz müsste zur Erreichung dieser Zwecke geeignet sein. Im Hinblick auf den diesbezüglich äußerst weiten Einschätzungsspielraum des Gesetzgebers ist von der Geeignetheit eines absoluten Verschlüsselungsverbots auszugehen:

Hauptanwendungsfall werden aber die herausgehobenen Teilgehalte des Rechts auf informationelle Selbstbestimmung und des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sein. Betroffen ist aber der Wesensgehalt des gesamten allgemeinen Persönlichkeitsrechts in der digitalen Welt.

„Im Rahmen der Eignungsprüfung ist nicht zu fordern, dass Maßnahmen, welche die angegriffene Norm erlaubt, stets oder auch nur im Regelfall Erfolg versprechen.“[904]

cc) Erforderlichkeit

Da zur Erreichung des unmittelbaren Ziels „Verhinderung des Einsatzes von Verschlüsselungsverfahren“ kein milderes Mittel ersichtlich ist, wäre ein absolutes Verschlüsselungsverbot auch erforderlich (s.o. unter I.1.3.c.cc)).

dd) Verhältnismäßigkeit im engeren Sinne

Schließlich müsste ein absolutes Verschlüsselungsverbotsgesetz auch verhältnismäßig im engeren Sinne sein:

„Dieses Gebot verlangt, dass die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen darf. Der Gesetzgeber hat das Individualinteresse, das durch einen Grundrechtseingriff beschnitten wird, den Allgemeininteressen, denen der Eingriff dient, angemessen zuzuordnen. Die Prüfung an diesem Maßstab kann dazu führen, dass ein Mittel nicht zur Durchsetzung von Allgemeininteressen angewandt werden darf, weil die davon ausgehenden Grundrechtsbeeinträchtigungen schwerer wiegen als die durchzusetzenden Belange.“[905]

(1) Durchsetzung gewichtiger Allgemeininteressen

Die im Wege eines absoluten Verschlüsselungsverbotes verfolgten Allgemeininteressen der Strafverfolgung, Verbrechensprävention sowie der Sicherung des Rechtsfriedens stellen gewichtige Rechtsgüter dar.

(2) Hohe Eingriffsintensität

Ein absolutes Verschlüsselungsverbotsgesetz stellt einen Grundrechtseingriff von hoher Intensität dar. Neben der besonderen *Quantität* der Maßnahme durch ihre Streubreite weist ein absolutes Verschlüsselungsverbot auch eine herausragende Eingriffs*qualität* auf. Dem Einzelnen wird untersagt, seine Daten und informationstechnischen Systeme durch den Einsatz von Verschlüsselungsverfahren selbst zu sichern. Dies erlaubt nicht nur dem Staat, im Einzelfall auf diese Daten zuzugreifen (soweit die Voraussetzungen einer entsprechenden Rechtsgrundlage für diesen Eingriff vorliegen). Vielmehr ermöglicht die unzureichende IT-Sicherheit es auch Kriminellen oder allen sonstigen interessierten Dritten, Daten auszuspähen oder zu ma-

904 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 222.
905 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 227.

nipulieren. In der Entscheidung zur „Online-Durchsuchung“ hat das BVerfG nochmals die besondere Gefährdungsqualität für die Persönlichkeit des Einzelnen durch die Bildung von Persönlichkeitsprofilen betont:

> „Der verfügbare Datenbestand kann detaillierte Informationen über die persönlichen Verhältnisse und die Lebensführung des Betroffenen, die über verschiedene Kommunikationswege geführte private und geschäftliche Korrespondenz oder auch tagebuchartige persönliche Aufzeichnungen umfassen. Ein staatlicher Zugriff auf einen derart umfassenden Datenbestand ist mit dem naheliegenden Risiko verbunden, dass die erhobenen Daten in einer Gesamtschau weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen ermöglichen.“[906]

Dies gilt nach dem BVerfG bereits bei einmaligen und nur punktuellen Zugriffen:

> „Eine staatliche Datenerhebung aus komplexen informationstechnischen Systemen weist ein beträchtliches Potential für die Ausforschung der Persönlichkeit des Betroffenen auf. Dies gilt bereits für einmalige und punktuelle Zugriffe wie beispielsweise die Beschlagnahme oder Kopie von Speichermedien solcher Systeme.“[907]

Dies gilt natürlich erst recht für eine längerfristige Überwachung.[908] Betroffen wären zudem auch Daten, die durch weitere, partiell privatsphärenrelevante Grundrechte (Meinungsfreiheit, Informationsfreiheit, Glaubens-, Bekenntnis- und Gewissensfreiheit, Versammlungsfreiheit, Vereinigungs- und Koalitionsfreiheit, Schutz von Ehe und Familie) geschützt sind. Im Wege der Schutzbereichsverstärkung ergibt sich daraus eine besondere Schwere des Eingriffs in das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG). Im Übrigen entsprechen die weiteren zu berücksichtigenden Gesichtspunkte den oben unter I.3.c.dd) genannten.

(3) Abwägung

Für die „Online-Durchsuchung“ hat das BVerfG entschieden, dass diese nur dann verhältnismäßig im engeren Sinne sei,

> „wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt.“[909]

Zwar ging es hierbei um den heimlichen Zugriff auf informationstechnische Systeme direkt durch die staatlichen Sicherheitsbehörden. Demgegenüber verfolgt ein absolutes Verschlüsselungsverbotsgesetz das Ziel, staatliche Ermittlungsmaßnahmen wie die Überwachung von E-Mail-Verkehr und Telekommunikation oder schlicht Hausdurchsuchungen nicht leer laufen zu lassen. Gleichwohl lassen sich aus der Entscheidung zur „Online-Durchsuchung“ Erkenntnisse hinsichtlich der verfas-

906 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 231 f.
907 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 230.
908 Vergleiche dazu nochmal ausführlich BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 235 ff.
909 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 242.

sungsrechtlichen Beurteilung eines absoluten Verschlüsselungsverbots ableiten. Die Implementierung der „Online-Durchsuchung“ ist maßgeblich der Tatsache des (befürchteten) zunehmenden Einsatzes von Verschlüsselungsverfahren geschuldet: Die Quellen-TKÜ etwa wird nur wegen der Existenz und Verbreitung von Internettelefonie-Programmen mit integrierter Verschlüsselung wie Skype benötigt. Über Optionen, mittels *`keyloggern´* Passwörter auszuspähen, wurde nur nachgedacht, weil immer mehr Menschen Daten auf ihren privaten PCs verschlüsselt und durch Passwort gesichert speichern. *Wenn also eine Umgehung oder Aushebelung von IT-Sicherheitsmaßnahmen im Einzelfall (Online-Durchsuchung) durch die staatlichen Sicherheitsbehörden bestimmten (verfassungsrechtlichen) Anforderungen genügen muss, dann müssen diese Anforderungen gleichermaßen gelten, wenn der Staat es dem Einzelnen von vornherein versagt, solche IT-Sicherheitsmaßnahmen zu treffen.*

Das BVerfG betont, dass schwer wiegende Grundrechtseingriffs *nur zum Schutz überragend wichtiger Rechtsgüter* vorgesehen werden können:[910]

> „Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen. Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existentielle Bedrohungslage nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen, durch die – wie hier – die Persönlichkeit des Betroffenen einer weitgehenden Ausspähung durch die Ermittlungsbehörde preisgegeben wird. Zum Schutz solcher Rechtsgüter hat sich der Staat auf andere Ermittlungsbefugnisse zu beschränken, die ihm das jeweils anwendbare Fachrecht im präventiven Bereich einräumt.“[911]

Es muss zudem nach der Rechtsprechung des BVerfG zumindest eine *hinreichende Wahrscheinlichkeit* dafür bestehen, dass tatsächlich eine Rechtsgutsbeeinträchtigung droht.[912] Dabei besteht zwar stets ein Abhängigkeitsverhältnis zwischen der Qualität der drohenden Rechtgutsbeeinträchtigung einerseits und der Wahrscheinlichkeit des Schadenseintritts andererseits (Relativität des Gefahrenbegriffs). Das BVerfG hat aber klargestellt, dass diese Relativität niemals so weit gehen kann, dass das Fehlen eines Teils dieses zweigeteilten Gefahrenbegriffs durch die überragende Qualität des anderen Teils ausgeglichen werden könnte:

> „Selbst bei höchstem Gewicht der drohenden Rechtsgutsbeeinträchtigung kann auf das Erfordernis einer hinreichenden Eintrittswahrscheinlichkeit nicht verzichtet werden. Auch muss als Voraussetzung eines schweren Grundrechtseingriffs gewährleistet bleiben, dass Annahmen

910 Dies hat das BVerfG für den Zugriff auf Telekommunikationsdaten in seiner Vorratsdatenspeicherungsentscheidung bestätigt; BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 227.

911 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 247 f.

912 Auch für den Zugriff auf im Rahmen der Vorratsdatenspeicherung gespeicherte Telekommunikationsdaten verlangt das BVerfG tatsächliche Anhaltspunkte für eine konkrete Gefhr, vgl. BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 231.

und Schlussfolgerungen einen konkret umrissenen Ausgangspunkt im Tatsächlichen besitzen."[913]

In diesem Zusammenhang betont das BVerfG nochmals die notwendige Einzelfallbezogenheit:

„Die konkrete Gefahr wird durch drei Kriterien bestimmt: den Einzelfall, die zeitliche Nähe des Umschlagens einer Gefahr in einen Schaden und den Bezug auf individuelle Personen als Verursacher. […] Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann."[914]

Diesen Vorgaben kann ein absolutes Verschlüsselungsverbotsgesetz nicht genügen, da es *alle Grundrechtsträger* in Deutschland betrifft und *generell* gilt. Das bedeutet, dass es erstens gerade nicht nur dem Schutz bestimmter überragend wichtiger Rechtsgüter dient, und zweitens, dass es nicht nur für konkrete Einzelfälle gilt. Zwar hat das BVerfG – etwa für die strategische Telekommunikationsüberwachung[915] – anerkannt, dass für Vorfeldmaßnahmen geringere Anforderungen an den Konkretisierungsgrad der Gefahr zu stellen sind. Auch hier hat das BVerfG aber wiederholt hervorgehoben, dass eine „globale und pauschale Überwachung" unzulässig sei (wegen Verstoßes gegen die Wesensgehaltsgarantie, Art. 19 II GG), und rechtliche und tatsächliche Begrenzungen für Überwachungsmaßnahmen verlangt:

„Eine "globale und pauschale Überwachung", die das Grundgesetz auch zu Zwecken der Auslandsaufklärung nicht zuließe, findet ebensowenig statt wie eine voraussetzungslose Erfassung sämtlicher Fernmeldekontakte bestimmter Grundrechtsträger. Vielmehr bleibt die Überwachung und Aufzeichnung des Fernmeldeverkehrs sowohl rechtlich als auch tatsächlich begrenzt."[916]

Diese rechtlichen und tatsächlichen Begrenzungen sah das BVerfG (größtenteils) für die strategische Telekommunikationsüberwachung (noch) als gegeben an:

„Eine Begrenzung folgt zunächst daraus, daß Gegenstand der Überwachung gemäß § 3 Abs. 1 Satz 1 G 10 nur der internationale nicht leitungsgebundene Verkehr ist. […] Innerhalb der internationalen nicht leitungsgebundenen Fernmeldekontakte wird die Erfassung weiter durch den Umstand gemindert, daß nach Auskunft des Sachverständigen Wiesbeck der sogenannte Uplink technisch nur begrenzt beobachtet werden kann, im wesentlichen also nur der sogenannte Downlink aufgefangen wird."[917]

Demgegenüber finden sich bei einem absoluten Verschlüsselungsverbot keinerlei Begrenzungen, es wirkt jederzeit, umfassend und gegenüber jedermann. Selbst zum Schutz überragender Rechtsgüter ist dies unverhältnismäßig:

„Die Verfassung verlangt vom Gesetzgeber, eine angemessene Balance zwischen Freiheit und Sicherheit herzustellen. Das schließt nicht nur die Verfolgung des Zieles absoluter Sicherheit

913 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 245.
914 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 251.
915 BVerfG, Urteil vom 14.07.1999, Az.: 1 BvR 2226/94 et al.
916 BVerfG, Urteil vom 14.07.1999, Az.: 1 BvR 2226/94 et al., Rn. 221.
917 BVerfG, Urteil vom 14.07.1999, Az.: 1 BvR 2226/94 et al., Rn. 222 und 224.

aus, welche ohnehin faktisch kaum, jedenfalls aber nur um den Preis einer Aufhebung der Freiheit zu erreichen wäre. Das Grundgesetz unterwirft auch die Verfolgung des Zieles, die nach den tatsächlichen Umständen größtmögliche Sicherheit herzustellen, rechtsstaatlichen Bindungen, zu denen insbesondere das Verbot unangemessener Eingriffe in die Grundrechte als Rechte staatlicher Eingriffsabwehr zählt. In diesem Verbot finden auch die Schutzpflichten des Staates ihre Grenze."[918]

4. Ergebnis

Ein absolutes Verschlüsselungsverbotsgesetz würde gegen das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) verstoßen, insbesondere in seinen Ausprägungen als Recht auf informationelle Selbstbestimmung und als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Zum einen würde ein solches absolutes Verbot den Wesens- und Menschenwürdegehalt des Rechts auf informationelle Selbstbestimmung sowie des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme antasten. Weiter wäre der Grundrechtseingriff durch ein absolutes Verschlüsselungsverbot von einer solchen Intensität, dass er selbst zum Schutz überragender Rechtsgüter nicht verfassungsrechtlich zu rechtfertigen wäre. Eine entsprechende Verfassungsänderung würde im Hinblick auf die Berührung des Menschenwürdegehalts an der Ewigkeitsgarantie (Art. 79 III GG i.V.m. Art. 1 I GG) scheitern.

IV. Zusammenfassung

Ein absolutes Verschlüsselungsverbotsgesetz verstößt gegen das Fernmeldegeheimnis (Art. 10 I GG), das Recht auf Unverletzlichkeit der Wohnung (Art. 13 I GG) sowie das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG). Soweit der Geltungsbereich des Fernmeldegeheimnisses eröffnet ist, ist dieses als lex specialis einschlägig. Im Übrigen wird ein Recht auf Verschlüsselung durch das allgemeine Persönlichkeitsrecht gewährleistet. Soweit es sich um Daten in der räumlichen Privatsphäre handelt, ist das Recht auf Unverletzlichkeit der Wohnung daneben anwendbar. Nach keiner der betroffenen Grundrechtsnormen kann ein Verschlüsselungsverbot verfassungsrechtlich gerechtfertigt werden, da ein solches sich insbesondere als unverhältnismäßig darstellt. Ein absolutes Verschlüsselungsverbot privater Daten wäre daher verfassungswidrig. Auch im Wege einer Verfassungsänderung könnte ein absolutes Verschlüsselungsverbot nicht eingeführt werden, da es in den unantastbaren Kernbereich privater Lebensgestaltung und damit den durch Art. 79 III GG dauerhaft gewährleisteten Menschenwürdegehalt eingreifen würde.

918 BVerfG, Beschluss vom 04.04.2006, Az.: 1 BvR 518/02, Rn. 128 f.

Daneben könnte sich ein absolutes Verschlüsselungsverbotsgesetz auch aus einer wirtschaftlichen Perspektive als verfassungswidrig erweisen; nicht nur, weil die wirtschaftliche Betätigungsfreiheit im Hinblick auf bestimmte Geschäftsfelder eingeschränkt wird, sondern darüber hinaus, weil umfassend der Schutz von Betriebs- und Geschäftsgeheimnissen erschwert, wenn nicht unmöglich gemacht wird. Bestimmte Berufszweige erweisen sich dabei als auch nach dem Grundgesetz besonders schutzwürdig (etwa die durch Art. 5 I S. 2 GG geschützte Presse oder die Forschungsfreiheit nach Art. 5 III GG, schließlich die Berufsgeheimnisträger wie etwa Geistliche).

I. Verstoß gegen die Eigentumsfreiheit (Art. 14 I S. 1 GG)

Ein absolutes Verschlüsselungsverbotsgesetz könnte gegen die Eigentumsfreiheit (Art. 14 I S. 1 GG) verstoßen. Ein Verstoß kommt unter folgenden vier Aspekten in Betracht:

- Zum einen könnte ein Verstoß gegen Art. 14 I S. 1 GG vorliegen, da Inhaber von Immaterialgüterrechten hinsichtlich Verschlüsselungsverfahren in ihren Verwertungsrechten beschränkt werden könnten.
- Des Weiteren könnten Verschlüsselungsverfahren auch Betriebs- und Geschäftsgeheimnisse darstellen und als solche von Art. 14 I S. 1 GG geschützt sein, sei es als Bestandteil eines Rechts am eingerichteten und ausgeübten Gewerbebetrieb, sei es als eigenständige Rechtsposition.
- Ein Eingriff in geschützte Betriebs- und Geschäftsgeheimnisse könnte weiter darin liegen, dass ein absolutes Verschlüsselungsverbot den Grundrechtsträgern die Implementierung effektiver Maßnahmen der IT-Sicherheit zum Schutz von Betriebs- und Geschäftsgeheimnissen untersagen würde.
- Soweit das jeweilige Geschäftsmodell wesentlich darauf basiert, Produkte via Internet zu vertreiben (hier im Folgenden als E-Commerce bezeichnet[919]), könnte dieses durch ein absolutes Verschlüsselungsverbot de facto zunichte gemacht werden. Auch hierin könnte ein Verstoß gegen die Eigentumsfreiheit liegen.

Hervorzuheben ist, dass im Bereich der Eigentumsfreiheit Verschlüsselungsverfahren nicht nur – wie durchgehend im Bereich der Privatsphärengewährleistungen der Fall – als *Mittel* zum Schutz bestimmter Daten geschützt sein könnten (*derivativer Schutz*), sondern Verschlüsselungsverfahren daneben auch *selbst Schutzgegen-*

919 Soweit ersichtlich gibt es keine eindeutige Definition des Begriffs „E-Commerce“. Im weiteren Sinne können alle Geschäftsprozesse, die ganz oder teilweise mittels elektronischer Kommunikationstechnologien abgewickelt werden, unter den Begriff subsumiert werden (vgl. insoweit nur Wikipedia, Elektronischer Handel, Version vom 13.07.2008, 21.11 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=Elektronischer_Handel&oldid=48347292). Hier wird unter „E-Commerce“ nur der E-Commerce im engeren Sinne verstanden.

stand der Eigentumsfreiheit sein könnten (*originärer Schutz*). Bei den ersten beiden der oben genannten Aspekte handelt es sich um einen solchen originären Schutz von Verschlüsselungsverfahren (als Immaterialgüterrechte bzw. als Betriebs- und Geschäftsgeheimnisse). Die beiden weiteren Aspekte sind dagegen wiederum Beispiele für den derivativen Schutz von Verschlüsselung.

1. Schutzbereich der Eigentumsfreiheit (Art. 14 I S. 1 GG)

Art. 14 I S. 1 GG gewährleistet den Schutz des Eigentums. Der Eigentumsbegriff ist dabei nicht von der Verfassung selbst vorgegeben; er muss vielmehr nach Art. 14 I S. 2 GG („Inhalt und Schranken werden durch die Gesetze bestimmt.“) durch den Gesetzgeber „normativ geschaffen“ werden.[920] Eigentum im Sinne des Art. 14 I S. 1 GG umfasst dabei nicht nur das Sacheigentum nach § 903 BGB, sondern auch andere vermögenswerte private oder subjektiv-öffentliche Rechte. Entscheidend ist die Funktionsäquivalenz dieser Rechtspositionen zum Sacheigentum.[921]

> „Voraussetzung des Schutzes nach Art. 14 GG ist, daß es sich […] um ein subjektives vermögenswertes Recht handelt, das dem Berechtigten von der objektiven Rechtsordnung ebenso ausschließlich wie Eigentum an einer Sache zur privaten Nutzung und zur eigenen Verfügung zugeordnet ist.“[922]

Daher fallen unter den Eigentumsbegriff des Art. 14 I S. 1 GG auch dingliche Rechte, sonstige absolut geschützte Rechtspositionen, Forderungen, „eigentumskräftig verfestigte Anspruchspositionen“[923] sowie Zugangs- und Nutzungsrechte.[924] Eine uneingeschränkte Verfügungsmacht ist nicht erforderlich.[925]

a. Schutz von Immaterialgüterrechten

Auch Immaterialgüterrechte wie Urheberrechte und Patente gehören zum durch Art. 14 I S. 1 GG geschützten Eigentum.[926] Verschlüsselungsverfahren können zunächst unter dem Aspekt Gegenstand des grundgesetzlichen Eigentumsschutzes sein, als sie in Computerprogrammen verwendet werden. Computerprogramme[927] können Ge-

920 *Wieland*, in: *Dreier,* GG, Art. 14, Rn. 25; *Ossenbühl*, Staatshaftungsrecht, S. 150; *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn. 50; BVerfGE 58, 300, 330 – Naßauskiesung.
921 *Wieland*, in: *Dreier,* GG, Art. 14, Rn. 31.
922 BVerfGE 78, 58, 71.
923 *Wieland*, in: *Dreier,* GG, Art. 14, Rn. 41.
924 *Ossenbühl*, Staatshaftungsrecht, S. 150.
925 *Wieland*, in: *Dreier,* GG, Art. 14, Rn. 34; *Ossenbühl*, Staatshaftungsrecht, S. 152; BVerfGE 83, 201, 209.
926 *Wieland*, in: *Dreier,* GG, Art. 14, Rn. 59 f.; *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn. 17.
927 Siehe ausführlich zum Begriff des Computerprogramms *Marly,* Praxishandbuch Softwarerecht, Rn. 1 ff, insbes. 8 ff.

genstand von Urheberrechten sein (§ 2 I Nr. 1 UrhG).[928] Nicht vom Schutz umfasst sind nach § 69a II S. 2 UrhG die „Ideen und Grundsätze, die einem Element eines Computerprogramms zugrunde liegen." Das heißt, dass die einem Computerprogramm zu Grunde liegenden mathematischen Prinzipien urheberrechtlichem Schutz nicht zugänglich sind.[929] Für Verschlüsselungsverfahren bedeutet dies, dass der (etwa dem RSA-Verfahren) zu Grunde liegende Algorithmus[930] nicht urheberrechtlich geschützt ist.[931] Die konkrete Implementierung von Verschlüsselungsalgorithmen innerhalb eines Computerprogramms ist aber schutzfähig. Geschützt werden vor allem die Form und die innere Gestaltung[932] – soweit sie über die erforderliche Schöpfungshöhe verfügen.[933] Grundsätzlich können Verschlüsselungsverfahren mithin Gegenstand urheberrechtlichen Schutzes und damit auch des verfassungsrechtlichen Eigentumsschutzes sein.

Computerprogramme als solche sind dagegen nicht patentfähig (§ 1 III Nr. 3 PatG).[934] Es muss vielmehr ein besonderer Zusammenhang mit der Lösung eines konkreten technischen Problems bestehen.[935] Dies kann etwa der Fall sein bei einer besonderen Einheit von Hard- und Softwarekomponenten.[936] Der BGH fragt in einer Gesamtbetrachtung nach dem Vorliegen der erforderlichen „Technizität":[937]

> „Ob eine auf ein Programm für Datenverarbeitungsanlagen gerichtete Patentanmeldung die erforderliche Technizität aufweist, ist auf Grund einer Gesamtbetrachtung des Anmeldungsgegenstands im Einzelfall festzustellen."[938]

928 *Marly,* Praxishandbuch Softwarerecht, Rn. 69 ff.

929 So auch Hoeren, Skript Internetrecht (Stand Feb. 2010), verfügbar unter: http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Internetrecht_Februar2010.pdf (30.03.2010), S. 111; *Marly,* Praxishandbuch Softwarerecht, Rn.83.

930 Zum Begriff des Algorithmus sowie der Abgrenzung zum Computerprogramm ausführlich *Marly,* Praxishandbuch Softwarerecht, Rn. 29 ff.

931 *Grützmacher*, in: *Wandtke/Bullinger,* UrhR, § 69a, Rn. 28. *Marly,* Praxishandbuch Softwarerecht, Rn. 86 weist darauf hin, dass die Gegenüberstellung der Begriffe Algorithmus einerseits und Computerprogramm andererseits für die Bestimmung der Grenzen urheberrechtlichen Schutzes unbrauchbar sei. Rechtsprechung und Literatur scheinen die Abgrenzung als Wertungsfrage im Einzelfall anzusehen. Jenseits dieser Abgrenzungs- und Terminologiefragen soll an dieser Stelle die grundsätzliche Erkenntnis ausreichen, dass mathematische Rechenverfahren an sich keinen urheberrechtlichen Schutz genießen, ihr konkreter Einsatz in einem Computerprogramm im Einzelfall aber durchaus schutzfähig sein kann.

932 *Grützmacher*, in: *Wandtke/Bullinger,* UrhR, § 69a, Rn. 23 ff.

933 Ausführlich zur „eigenen geistigen Schöpfung" *Marly,* Praxishandbuch Softwarerecht, Rn. 90 ff.

934 *Marly,* Praxishandbuch Softwarerecht, Rn. 395; Hoeren, Skript Internetrecht (Stand Sept. 2009), verfügbar unter: http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_September2009.pdf (05.06.2009), S. 226.

935 *Mes,* PatentG, § 1, Rn. 83 f.; *Marly,* Praxishandbuch Softwarerecht, Rn. 398.

936 *Mes,* PatentG, § 1, Rn. 85.

937 Vgl. insoweit ausführlich zur Rechtsprechung *Mes,* PatentG, § 1, Rn. 89 ff. sowie *Marly,* Praxishandbuch Softwarerecht, Rn. 396 ff. Vgl. zur Technizität auch jüngst BGH, Urteil vom 20.01.2009, Az.: X ZB 22/02.

938 BGH, NJW 2000, 1953, 1955.

Somit können im Einzelfall Verschlüsselungsverfahren auch als Bestandteile von Computerprogrammen zur Lösung einer konkreten technischen Fragestellung als Patente durch die Eigentumsgarantie des Art. 14 I S. 1 GG geschützt sein.

b. Schutz von Betriebs- und Geschäftsgeheimnissen?

Zu prüfen ist, ob Art. 14 I S. 1 GG über den Schutz von Rechten des geistigen Eigentums hinaus auch weiteres unternehmerisches Wissen in Form von Betriebs- und Geschäftsgeheimnissen schützt. In der Literatur scheint dies ohne Weiteres angenommen zu werden.[939]

aa) Betriebs- und Geschäftsgeheimnisse als Eigentum?

Die Bestimmung des im Wege des Art. 14 I S. 1 GG geschützten Eigentums ergibt sich aus einer Gesamtschau der zivil- wie öffentlich-rechtlichen Vorschriften, die Aussagen über die Zuordnung vermögenswerter Rechte treffen.[940] Betriebs- und Geschäftsgeheimnisse sind in vielerlei Normen geschützt, etwa § 6 I S. 2 Informationsfreiheitsgesetz, § 9 I S. 1 Nr. 3 Umweltinformationsgesetz, § 17a I S. 1 Gentechnikgesetz, § 22 II S. 1 Chemikaliengesetz. Strafrechtliche Normen wie § 17 I, II UWG, § 85 I GmbHG, § 404 I AktG, § 151 I GenG, § 333 I HGB, § 120 I BetrVG und § 203 StGB bestätigen diesen Schutz und sichern ihn für bestimmte Bereiche mittels strafrechtlicher Sanktionen ab. Der Einsatz des stärksten staatlichen Instruments zum Schutz von Grundrechten, des Strafrechts, zeigt die Bedeutung des Schutzes von Betriebs- und Geschäftsgeheimnissen.

Eine Legaldefinition des Betriebs- und Geschäftsgeheimnisses in öffentlich-rechtlichen Normen existiert nicht, so dass auf Rechtsprechung und Literatur zu § 17 UWG

> „(1) Wer als eine bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
>
> (2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen,
>
> 1. sich ein Geschäfts- oder Betriebsgeheimnis durch

939 Vgl. *Manssen*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 12, Rn. 289, nach dessen Auffassung der Schutz von Betriebs- und Geschäftsgeheimnissen vor allem durch Art. 14 GG gewährleistet wird – ohne dass diese Auffassung näher diskutiert oder begründet würde; *Piper/Ohly,* UWG, vor § 17, Rn. 8 m.w.N.; *Berg,* GewArch 1996, 177, 178.

940 *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 111 und 113.

a) Anwendung technischer Mittel,

b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder

c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist, unbefugt verschafft oder sichert oder

2. ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten Mitteilungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt."

zurückgegriffen wird.[941] Demzufolge sind unter Betriebs- und Geschäftsgeheimnissen solche

„Tatsachen zu verstehen, die nach dem erkennbaren Willen des Betriebsinhabers geheim gehalten werden sollen, die ferner nur einem begrenzten Personenkreis bekannt und damit nicht offenkundig sind und hinsichtlich derer der Betriebsinhaber deshalb ein berechtigtes Geheimhaltungsinteresse hat, weil eine Aufdeckung der Tatsachen geeignet wäre, dem Geheimnisträger wirtschaftlichen Schaden zuzufügen."[942]

Auf diese Definition hat der Gesetzgeber etwa in § 6 I S. 2 IFG abgestellt, wie sich aus der Begründung des Gesetzesentwurfs ergibt.[943] Demnach müssen für das Vorliegen eines Betriebs- oder Geschäftsgeheimnisses folgende Voraussetzungen erfüllt sein: erkennbarer Geheimhaltungswille des Betriebsinhabers, keine Offenkundigkeit sowie ein berechtigtes Geheimhaltungsinteresse.

Daraus ergibt sich, dass es sich bei Betriebs- und Geschäftsgeheimnissen um Rechtspositionen handelt, die durch Art. 14 I S. 1 GG geschützt werden: Nach der Rechtsprechung des BVerfG (s.o.) werden von der Eigentumsgarantie vermögenswerte Rechte geschützt, die dem Berechtigten von der objektiven Rechtsordnung ebenso ausschließlich wie Eigentum zur eigenen Verfügung zugeordnet sind. Wie die obige Definition von Betriebs- und Geschäftsgeheimnissen zeigt, handelt es sich dabei um *vermögenswerte Rechtspositionen*, da Betriebs- und Geschäftsgeheimnisse qua definitionem wirtschaftlichen Wert haben (da eine Aufdeckung geeignet sein muss, dem Geheimnisträger wirtschaftlichen Schaden zuzufügen, vgl. oben). Diese vermögenswerten Rechtspositionen sind auch *ausschließlich dem Betriebsinhaber zur eigenen Verfügung zugeordnet*. Soweit Betriebsangehörige ebenfalls Kenntnis von Betriebs- und Geschäftsgeheimnissen haben, stehen ihnen gerade nicht die Verfügungs- und Verwertungsbefugnisse zu. § 17 UWG stellt umfassend die unbefugte Mitteilung (§ 17 I UWG), die unbefugte Verschaffung und Sicherung (§ 17 II Nr. 1 UWG) sowie die unbefugte Verwertung oder Mitteilung von unbefugt verschafften oder gesicherten Betriebs- und Geschäftsgeheimnissen (§ 17 II Nr. 2 UWG) unter Strafe. Einzig die unbefugte Verwertung von Betriebs- und Geschäftsgeheimnissen, die weder unbefugt erlangt noch unbefugt gesichert wurden, wird nicht strafrechtlich geahndet, regelmäßig aber über zivilrechtliche Wettbewerbsvereinbarungen abgesi-

941 So *Berg,* GewArch 1996, 177, 178, allerdings ohne weitere Nachweise.
942 BGH, Urteil vom 10.05.1995, Az.: 1 StR 764/94, NJW 1995, 2301.
943 Vgl. BT-Drs. 15/4493, S. 14.

chert.[944] Daher sind Betriebs- und Geschäftsgeheimnisse von der objektiven Rechtsordnung dem Betriebsinhaber zur ausschließlichen Verfügung zugeordnet und folglich Gegenstand der Eigentumsgarantie des Art. 14 I S. 1 GG.[945]

Verschlüsselungsverfahren können mithin auch als Betriebs- und Geschäftsgeheimnisse in den Schutzbereich des Art. 14 I S. 1 GG fallen.

bb) Schutz von Betriebs- und Geschäftsgeheimnissen durch Verschlüsselung?

Daneben können Verschlüsselungsverfahren aber nicht nur selbst Betriebs- und Geschäftsgeheimnisse darstellen oder Bestandteil davon sein, sondern vor allem dazu dienen, andere Betriebs- und Geschäftsgeheimnisse effektiv vor fremder Kenntnisnahme zu schützen.[946] Auch insoweit steht ein gestiegenes Gefährdungspotential zunehmenden staatlichen Schutzdefiziten gegenüber.[947] Das veränderte Gefährdungspotential ergibt sich vor allem aus folgenden vier Faktoren:

- Der Einsatz von Informationstechnologie (IT) nimmt gerade auch im Wirtschaftsleben eine zunehmend bedeutende Rolle ein. Längst nicht mehr nur im Bereich des E-Commerce durchdringt die Nutzung von IT das Geschäftsleben nahezu vollständig.[948]
- Daraus ergeben sich Angriffsmöglichkeiten zum einen auf immer mehr Wirtschaftsakteure, zum anderen auf immer mehr Prozesse: Je mehr die innerbetriebliche Organisation und Kommunikation sowie die externen Kontakte auf dem Einsatz von IT basieren, desto stärker wird die Gesamtbedeutung funktionierender IT für ein Unternehmen.[949]
- Ein Verzicht auf den Einsatz von Informations- und Kommunikationstechnologien dürfte keine Lösungsoption darstellen. Zum einen erwarten Kunden und Geschäftspartner mit zunehmender Sozialüblichkeit die Nutzung von Informations- und Kommunikationstechnologien im Wirtschaftsverkehr. Zum anderen dürfte sich der Wegfall der Rationalisierungs- und Synergieeffekte, die durch

944 Dabei handelt es sich um die Fälle, in denen Betriebsangehörige während und vor allem nach ihrer Beschäftigungszeit Betriebs- und Geschäftsgeheimnisse verwerten, die ihnen in Erinnerung geblieben sind. Letztere Einschränkung ist bedeutsam, denn jede als Gedächtnisstütze angefertigte Aufzeichnung, Kopie etc. würde bereits eine „Sicherung" bedeuten; vgl. *Piper/Ohly,* UWG, § 17, Rn. 19; *Hefermehl/Köhler/Bornkamm,* UWG, § 17, Rn. 34.

945 So auch *Berg,* GewArch 1996, 177, 178.

946 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 183.

947 Vgl. zu den zunehmenden staatlichen Schutzdefiziten oben unter A.III.1.d.bb).

948 Siehe zur zunehmenden Bedeutung von IT wie elektronischer Kommunikation *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 183.

949 Die gestiegene Bedeutung zeigt sich etwa daran, dass Abschlussprüfer im Rahmen der Jahresabschlussprüfung bei der Prüfung der Einhaltung der Grundsätze ordnungsgemäßer Buchführung auch die (rechnungslegungsbezogenen) IT-Systeme prüfen bzw. mit der Umsetzung der Euro-SOX-Richtlinien in nationales Recht prüfen müssen; vgl. dazu Prüfungsstandard des Instituts der Wirtschaftsprüfer in Deutschland IDW PS 330 sowie *Heckmann,* MMR 2006, 280, 284.

den Einsatz von Informationstechnologien in Unternehmensprozessen bewirkt werden, als enormer Wettbewerbsnachteil im internationalen Markt manifestieren.

- Gleichzeitig besteht nach Erkenntnissen des Verfassungsschutzes ein außerordentliches Interesse etwa an technischen Innovationen von Seiten ausländischer Nachrichtendienste.[950] Neben der Konkurrenzausspähung[951] durch andere (ev. konkurrierende) Unternehmen besteht daher für Unternehmen die manifeste Gefahr von Wirtschaftsspionage[952] durch extrem ressourcenstarke Akteure. Ziele der Spionage können Daten, Ideen, Entscheidungen, Strategien etc. während des gesamten Entstehungs- und Vermarktungsprozesses eines Wirtschaftsguts sein.[953] Angriffen auf die IT oder mittels IT kommt dabei besondere Bedeutung zu.[954] Schließlich setzen viele Staaten Systeme der strategischen Überwachung

950 Siehe Verfassungsschutzbericht Baden-Württemberg 2007, verfügbar unter: http://www.sicherheitsforum-bw.de/x_loads/jabe-spio-2007.pdf (28.07.2008), S. 242:„Deutsche Firmen stellen aufgrund ihrer hohen Leistungen im Bereich Produktinnovation ein überdurchschnittlich attraktives Ziel für fremde Nachrichtendienste dar".

951 Nach Bayerisches Landesamt für Verfassungsschutz/Landesamt für Verfassungsschutz Baden-Württemberg, Wirtschaftsspionage in Baden-Württemberg und Bayern, verfügbar unter: http://www.sicherheitsforum-bw.de/x_loads/wirtschaftsspionage-2006.pdf (28.07.2008), S. 9 „versteht man unter Konkurrenzausspähung die Ausforschung, die ein (konkurrierendes) Unternehmen gegen ein anderes betreibt".

952 Als Wirtschaftsspionage definieren Bayerisches Landesamt für Verfassungsschutz/Landesamt für Verfassungsschutz Baden-Württemberg, Wirtschaftsspionage in Baden-Württemberg und Bayern, verfügbar unter: http://www.sicherheitsforum-bw.de/x_loads/wirtschaftsspionage-2006.pdf (28.07.2008), S. 9 „die staatliche gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben".

953 Vgl. im Einzelnen Bayerisches Landesamt für Verfassungsschutz/Landesamt für Verfassungsschutz Baden-Württemberg, Wirtschaftsspionage in Baden-Württemberg und Bayern, verfügbar unter: http://www.sicherheitsforum-bw.de/x_loads/wirtschaftsspionage-2006.pdf (28.07.2008), S. 27. Einer Studie von McAfee zufolge sollen allein 2008 Schäden aus Datenlecks und Diebstählen von geistigem Eigentum in Höhe von einer Billion Dollar weltweit entstanden sein; heise online vom 29.01.2009, Studie: Krise verstärkt Gefahr von Datendiebstahl, verfügbar unter: http://www.heise.de/newsticker/Studie-Krise-verstaerkt-Gefahr-von-Datendiebstahl--/meldung/126 565 (30.01.2009).

954 *Koch,* CR 1997, 106, 107 f.; vgl. weiter ausführlich dazu Bayerisches Landesamt für Verfassungsschutz/Landesamt für Verfassungsschutz Baden-Württemberg, Wirtschaftsspionage in Baden-Württemberg und Bayern, verfügbar unter: http://www.sicherheitsforum-bw.de/x_loads/wirtschaftsspionage-2006.pdf (28.07.2008), S. 31 ff.; Verfassungsschutzbericht Baden-Württemberg 2007, verfügbar unter: http://www.sicherheitsforum-bw.de/x_ loads/jabe-spio-2007.pdf (28.07.2008), S. 244.

des Internet- und E-Mail-Verkehrs ein (Russland, USA, Großbritannien,[955] neuerdings auch Schweden[956] etc.).[957]

Dieser gestiegenen Bedeutung sicherer IT und dem veränderten Gefährdungspotential steht ein zunehmendes Schutzdefizit gegenüber. Der Staat ist de facto nicht in der Lage, rechtlichen oder tatsächlichen Schutz vor Angriffen auf Informations- und Kommunikationstechnologien zu gewährleisten. Schutz kann insoweit nur ein umfassendes Informationsschutzkonzept bieten:

> „Das wirksamste Mittel gegen die illegale Nutzung des eigenen Wissens durch fremde Staaten, Konkurrenzunternehmen oder Einzelpersonen bietet ein umfassendes Informationsschutzkonzept. Jedoch garantiert nur die Kombination sorgfältig aufeinander abgestimmter personeller, organisatorischer sowie materieller Maßnahmen eine adäquate Schutzwirkung. Der Verzicht auf einen der genannten Bestandteile führt zwangsläufig zu Sicherheitslücken."[958]

Ein derartiges Informationsschutzkonzept muss notwendig ein IT-Sicherheitskonzept beinhalten. IT-Sicherheit ist nach derzeitigem Stand der Technik ohne Verschlüsselungsverfahren nicht realisierbar. Daher muss der grundrechtliche Schutz von Betriebs- und Geschäftsgeheimnissen ein Recht auf Verschlüsselung gewährleisten:

> „Die Nutzung unterschiedlicher Erscheinungsformen des electronic commerce setzt den Zugriff auf sichere Verschlüsselungsverfahren voraus – und zwar sowohl für die Angebots- als auch für die Nachfrageseite."[959]

Gleiches gilt auch für den Schutz des geistigen Eigentums. Marken- und Produktpiraterie kann nicht allein durch rechtliche, sondern vor allem in Kombination mit weiteren technischen und strategischen Maßnahmen entgegengewirkt werden, wie eine jüngere Studie des Frauenhofer-Instituts für Produktionstechnologie zeigt.[960] Der Einsatz von Sicherheitstechnologie stellt danach die mit Abstand wichtigste Maßnahme zum Schutz vor Produktimitationen dar. Der Schutz unternehmerischen

955 Einzelheiten zu den drei Genannten Bayerisches Landesamt für Verfassungsschutz/Landesamt für Verfassungsschutz Baden-Württemberg, Wirtschaftsspionage in Baden-Württemberg und Bayern, verfügbar unter: http://www.sicherheitsforum-bw.de/x_loads/wirtschaftsspionage-2006.pdf (28.07.2008), S. 37.

956 heise online vom 18.06.2008, Widerstand gegen umfassendes Abhörgesetz in Schweden, verfügbar unter: http://www.heise.de/newsticker/Widerstand-gegen-umfassendes-Abhoergesetz-in-Schweden--/meldung/109644 (25.6.2008)

957 Für einen umfassenden Überblick über die Situation in einzelnen Ländern siehe Reporters sans frontières, The Internet under surveillance 2004, verfügbar unter: http://www.rsf.org/rubrique.php3?id_rubrique=433 (08.08. 2008).

958 Verfassungsschutzbericht Baden-Württemberg 2007, verfügbar unter: http://www.sicherheitsforum-bw.de/x_loads/jabe-spio-2007.pdf (28.07.2008), S. 250.

959 *Marauhn,* KritV 1999, 57, 77, der allerdings nur die Betroffenheit des E-Commerce sieht und dabei die Auswirkungen auf sonstige Wirtschaftsunternehmen übersieht.

960 Fraunhofer-Institut für Produktionstechnologie, Unternehmen handeln zu spät, verfügbar unter: http://www.produktpiraterie.fraunhofer.de/Zum_Thema2.htm (12.08.2008).

Know-hows erfordert daher zwingend ein wirksames Informationsschutz- und insbesondere IT-Sicherheitskonzept.[961]

c. Schutz des Rechts am eingerichteten und ausgeübten Gewerbebetrieb?

Ob über den Schutz der Betriebs- und Geschäftsgeheimnisse hinaus auch ein Recht am eingerichteten und ausgeübten Gewerbebetrieb im Schutzbereich des Art. 14 I S. 1 GG anzuerkennen ist, ist in der Literatur nach wie vor umstritten.[962] Das BVerfG hat die Frage in seiner Rechtsprechung bisher explizit offen gelassen.[963] Der Schutz des Gewerbebetriebs kann nach Ansicht des BVerfG jedenfalls nicht weiter reichen als der Schutz, den seine wirtschaftliche Grundlage genießt.[964] Umsatz- und Gewinnchancen, günstige tatsächliche oder rechtliche Gegebenheiten, bestehende Geschäftsverbindungen und Kundenstamm werden daher nach der Rechtsprechung des BVerfG nicht von der Eigentumsgarantie umfasst:[965]

> „Diese Chancen und Gegebenheiten sind für das Unternehmen von erheblicher, eigentumsrechtlich aber nur mittelbarer Bedeutung; sie entscheiden mit über das Risiko eines Unternehmers, seine Leistungen und Erzeugnisse rentabel abzusetzen, werden von der Rechtsordnung aber nicht dem geschützten Bestandswert des einzelnen Unternehmens zugeordnet. Beruhen solche, dem Unternehmer wirtschaftlich günstige Gegebenheiten und Chancen auf einer bestimmten Rechtslage und wird diese Rechtslage zum Nachteil der wirtschaftlichen Aussichten eines Unternehmers geändert, so bedeutet das eine Neuordnung der sozialen Bedingungen, innerhalb deren der Unternehmer seine Tätigkeit ausüben kann. Vor Art. 14 Abs. 1 Satz 2 GG ist dies so lange bedenkenfrei, als dadurch der Kern des Eigentumsrechts nicht angetastet wird.“[966]

Bloße Zukunftshoffnungen und Verdienstaussichten werden somit nicht durch Art. 14 I S. 1 GG geschützt, denn die Eigentumsgarantie umfasst nur das bereits Erworbene;[967] Erwerbs*möglichkeiten* werden allenfalls im Rahmen der Berufsfreiheit (Art. 12 I GG) gewährleistet:

> „Art. 14 Abs. 1 GG schützt das Erworbene, das Ergebnis der Betätigung, Art. 12 Abs. 1 GG dagegen den Erwerb, die Betätigung selbst. Greift somit ein Akt der öffentlichen Gewalt eher

961 Die Bedeutung der Kryptographie zum Schutz vor Industriespionage ebenfalls betonend *Andrzejak*, Kryptoregulierung, in: *Hoeren/Queck,* Rechtsfragen der Informationsgesellschaft, S. 132, 132.

962 Für den Schutz des Rechts am eingerichteten und ausgeübten Gewerbebetrieb vgl. ausführlich *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 132; *Ossenbühl*, Staatshaftungsrecht, S. 160 ff.; kritisch dazu *Wieland*, in: *Dreier,* GG, Art. 14, Rn. 50 ff. sowie *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn. 18.

963 BVerfGE 68, 193, 222; BVerfG, Beschluss vom13.06.2002, Az.: 1 BvR 482/02, Rn. 6; Beschluss vom 26.06.2002, Az.:1 BvR 558/91 und 1428/91, Rn. 76; Beschluss vom 28.07.2004, Az.: 1 BvR 2566/95, Rn. 40; Beschluss vom 24.11.2004, Az.: 1 BvR 1306/02, Rn. 15.

964 BVerfGE 58, 300, 353; *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 135.

965 *Wieland*, in: *Dreier,* GG, Art. 14, Rn. 50.

966 BVerfGE 45, 142, 173.

967 *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 99.

in die Freiheit der individuellen Erwerbs- und Leistungstätigkeit ein, so ist der Schutzbereich des Art. 12 Abs. 1 GG berührt; begrenzt er mehr die Innehabung und Verwendung vorhandener Vermögensgüter, so kommt der Schutz des Art. 14 GG in Betracht."[968]

aa) Abgrenzung von zukünftigen Erwerbschancen und bereits erworbenem Vermögensbestand

Insofern ist hier die Frage zu beantworten, ob Hersteller und Anbieter von Verschlüsselungsprodukten ebenso wie Unternehmer im Bereich des E-Commerce durch ein absolutes Verschlüsselungsverbotsgesetz in ihren zukünftigen Erwerbschancen oder in ihrem in der Vergangenheit erworbenen Vermögensbestand betroffen sind. Wurde ein derartiges Unternehmen bisher noch nicht betrieben, ist offensichtlich nur zukünftige Erwerbstätigkeit tangiert, mithin allein die Berufsfreiheit (Art. 12 I GG) betroffen.[969] Handelt es sich um bereits bestehende Unternehmen, kann auch der Schutzbereich des Art. 14 I S. 1 GG eröffnet sein – unabhängig davon, ob man ein eigenständiges Recht am eingerichteten und ausgeübten Gewerbebetrieb anerkennen möchte oder nicht. Die einzelnen Rechtspositionen, die in ihrer Gesamtheit das wirtschaftliche Unternehmen ausmachen, genießen jedenfalls den Schutz der Eigentumsgarantie. Auf die Frage, ob das Unternehmen über die Sach- und Rechtsgesamtheit der „Produkte, Sachanlagen, Betriebsgrundstücke, Forderungen, Finanzvermögen, laufende Vertragsbeziehungen, geistiges Eigentum"[970] und Betriebs- und Geschäftsgeheimnisse hinaus einen schützenswerten „spezifischen Mehrwert"[971] besitzt, kommt es dabei nicht an, da bereits hinsichtlich der das Unternehmen konstituierenden Einzelrechtspositionen der Schutzbereich eröffnet ist.

bb) Rechtliche Rahmenbedingung oder Substanzeingriff?

Geht es wie hier um die Auswirkungen veränderter gesetzlicher Regelungen auf ein bestehendes wirtschaftliches Unternehmen, ist bisher durch Rechtsprechung und Literatur nicht zufriedenstellend gelöst,[972] wann lediglich eine Veränderung der (rechtlichen) Rahmenbedingungen vorliegt, die nicht zum geschützten Bestand eines Un-

968 BVerfGE 30, 292, 335.
969 So auch für ein Verbot der Errichtung neuer Kernkraftwerke *Stüer/Loges,* NVwZ 2000, 9, 12 sowie *Stoll*, Sicherheit als Aufgabe von Staat und Gesellschaft, S. 175.
970 Aufzählung nach *Ossenbühl*, Staatshaftungsrecht, S. 161.
971 *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 132.
972 Auch *Ossenbühl*, Staatshaftungsrecht, S. 162 sieht hier „kaum lösbare Abgrenzungsprobleme".

ternehmens gehören (s.o.), und wann ein eigentumsrechtlich relevanter Eingriff in die Substanz des Gewerbebetriebs vorliegt.[973]

(1) Rechtliche Rahmenbedingung

In der jüngeren Entscheidung des BVerfG zu den landesrechtlichen Nichtraucherschutzgesetzen wurden die Rauchverbote allein an der Berufsausübungsfreiheit (Art. 12 I GG),[974] nicht aber an der Eigentumsfreiheit nach Art. 14 I S. 1 GG gemessen, obwohl das BVerfG selbst ausführlich auf die wirtschaftlichen Auswirkungen der Nichtraucherschutzgesetze für die Gaststättenbetreiber eingegangen ist.

> „An der Eigentumsgarantie (Art. 14 Abs. 1 GG) ist das Rauchverbot hingegen nicht zu messen. Zwar berührt es auch das durch Art. 14 Abs. 1 GG geschützte Hausrecht, der Schwerpunkt des Eingriffs liegt jedoch nicht in der Begrenzung der Innehabung und Verwendung dieser Vermögensposition, sondern in der Beschränkung der individuellen Erwerbs- und Leistungstätigkeit des Gastwirts. Der Schutz der Eigentumsgarantie kommt hier daher nicht in Betracht."[975]

Die Veränderung der Rahmenbedingungen wirtschaftlicher Tätigkeit fällt damit regelmäßig nicht in den Schutzbereich von Art. 14 I S. 1 GG. Ein Anspruch auf Fortbestand einer Gesetzeslage besteht nicht.[976] Wie *Bryde* betont, werden nur solche Vorteile rechtlich geschützt, auf deren Fortbestand der Betriebsinhaber vertrauen kann.[977] Darunter fallen gerade nicht Lagevorteile, eine günstige Gesetzeslage, eine widerrufliche öffentlich-rechtliche Konzession oder Genehmigung, die Einführung eines Anschluss- und Benutzungszwangs, auch wenn sie einem Unternehmen die Existenzgrundlage entzieht.[978] Dies sei laut *Bryde* Ausdruck einer freien Wirtschaftordnung, die dem Unternehmer erlaube, „sich auf günstige tatsächliche oder rechtliche Vorgaben einzustellen, aber er tut das auf eigenes Risiko."[979]

(2) Substanzeingriff

Umgekehrt scheint Einigkeit in der Literatur zu herrschen, dass die nachträgliche Befristung atomrechtlicher Betriebsgenehmigungen mit anschließender Stilllegung der Kernkraftwerke und einem entsprechenden Genehmigungsverbot für die Zukunft

973 Auch die in BVerfGE 30, 292, 335 vom BVerfG getroffenen Unterscheidung zwischen einer Betroffenheit „in ihrer Eigenschaft als Unternehmer" und einer Betroffenheit „in ihrer Eigenschaft als Eigentümer eines Unternehmens" ist insoweit wenig hilfreich.

974 BVerfG, Urteil vom 30.07.2008, Az.: 1 BvR 3262/07 et al., Rn. 92 ff.

975 BVerfG, Urteil vom 30.07.2008, Az.: 1 BvR 3262/07 et al., Rn. 91.

976 *Stüer/Loges,* NVwZ 2000, 9, 12.

977 *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn. 20.

978 So *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn. 20; vgl. dazu auch BGH, Beschluss vom 10.11.1975, NJW 1976, 520 mit vielen weiteren Beispielen sowie die Beispiele bei *Ossenbühl*, Staatshaftungsrecht, S. 163.

979 *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn. 20.

(sog. Atomausstieg) einen Eingriff in die Eigentumsgarantie des Art. 14 I S. 1 GG darstellen würde.[980] Auch wenn zur Begründung dieses Ergebnisses teilweise auf die öffentlich-rechtliche Genehmigung als eigentumsrechtlich geschützte Rechtsposition hingewiesen wird,[981] ist

> „zwischen der öffentlich-rechtlichen Rechtsstellung einerseits und der auf ihrer Grundlage auf Grund der eigenen Leistung aufgebauten Vermögensposition andrerseits zu unterscheiden."[982]

Grund des Eigentumsschutzes kann nur die durch eigene Leistung erworbene Stellung sein.[983] Die Berufsstellung auf Grund öffentlich-rechtlicher Zulassung unterscheidet sich insofern durch nichts von sonstigen Berufsstellungen. Die öffentlich-rechtliche Zulassung hat lediglich die Basis geboten, auf der die Berufsstellung erworben werden konnte. Dabei führt das Vorhandensein einer öffentlich-rechtlichen Genehmigung tatsächlich gar nicht zu einer Verstärkung des Grundrechtsschutzes;[984] vielmehr kann bei einem rechtmäßigen Widerruf oder auslaufender Befristung hiergegen gerade *kein* Eigentumsschutz geltend gemacht werden.[985] Festzuhalten ist, dass der einhellig angenommene Schutz der Atomanlagenbetreiber nicht auf die öffentlich-rechtliche Genehmigung der Anlage zurückzuführen ist. Insofern bleibt es beim „Substanzeingriff" als entscheidendem Kriterium für den Eigentumsschutz bestehender wirtschaftlicher Unternehmen.

Folgende mögliche Kriterien für die Bestimmung eines Substanzeingriffs können insoweit ausgemacht werden:

- Ein Substanzeingriff könnte vorliegen, wenn die Verfügungsbefugnis über das Eigentum zwar nicht unbedingt de jure, aber doch de facto abgeschafft wird, da sie wirtschaftlich sinnvoll nicht realisiert werden kann:[986]

  > „Eigentum i.S. des Art. 14 GG ist in seinem rechtlichen Gehalt durch Privatnützigkeit und grundsätzliche Verfügungsbefugnis über den Eigentumsgegenstand gekennzeichnet. Die Verfügungsbefugnis ist betroffen, wenn der Gesetzgeber eine Regelung trifft, die zwar die Möglichkeit der Veräußerung des geschützten Eigentumsgegenstandes nicht ausdrücklich verbietet,

980 *Stüer/Loges,* NVwZ 2000, 9, 12; *Stoll*, Sicherheit als Aufgabe von Staat und Gesellschaft, S. 179 sowie – ohne die Einschlägigkeit von Art. 14 I S. 1 GG näher zu diskutieren *Koch/Roßnagel,* NVwZ 2000, 1, 5 und *Detjen,* Forum Recht Online 2000.

981 Vgl. etwa *Stüer/Loges,* NVwZ 2000, 9, 12 und 13: "Der Betreiber eines Kernkraftwerks hat im Vertrauen auf den Bestand seiner gefestigten öffentlich-rechtlichen Position aus der Betriebsgenehmigung und unter Berücksichtigung der engen Widerrufs- bzw. Rücknahmemöglichkeiten des § 17 AtG seine Investitionsentscheidung getroffen." Dagegen sieht *Stoll*, Sicherheit als Aufgabe von Staat und Gesellschaft, S. 170 vor allem das Grundeigentum am Anlagengrundstück in seiner durch die öffentlich-rechtliche Genehmigung ausgestalteten Nutzung als durch Art. 14 I S. 1 GG geschützte Rechtsposition an.

982 *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 172.

983 *Wieland*, in: *Dreier,* GG, Art. 14, Rn. 64.

984 *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn. 30.

985 So überzeugend *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 172.

986 Andererseits differenziert etwa *Ossenbühl*, Staatshaftungsrecht, S. 152 gerade zwischen der Substanz des Eigentums und der Verfügungsbefugnis: „Geschützt ist das Eigentum in seiner Substanz. Die Verfügungsbefugnis des Eigentümers kann beschränkt werden. Aber `der Kern des Eigentumsrechts´ darf nicht angetastet werden."

aber sich diese Veräußerung als wirtschaftlich sinnvoll nicht realisierbar erweist. Eine gesetzliche Stillegungsanordnung von Kernkraftwerken führt zu ihrer Wertlosigkeit und ist ein Eingriff in die Verfügungsbefugnis und damit in die Substanz."[987]

- Ein Substanzeingriff könnte vorliegen, wenn – in Anlehnung an die soeben dargestellt Argumentation – die eigentumsrechtliche Position zwar normativ noch besteht, inhaltlich aber ausgehöhlt und entwertet ist, da die formale Position materiell nicht mehr sinnvoll genutzt werden kann (Aushöhlungs- oder Entwertungskriterium). Zwar garantiert die Eigentumsgarantie eigentlich gerade nur den Bestand des Eigentums und nicht den Wert, nach einer Meinung in der Literatur ist der Wertverlust aber zumindest ein Indiz für eine Rechtsgutsbeeinträchtigung:

  „Art. 14 garantiert grundsätzlich nur den Bestand, nicht den Tauschwert eines vermögenswerten Rechts, ohne daß der Tauschwert jedoch für die Eigentumsgarantie bedeutungslos wäre. Er ist vielmehr von Bedeutung für die Entschädigung rechtmäßiger wie rechtswidriger Eigentumsverkürzungen, und durch rechtswidriges Hoheitshandeln verursachte Wertverluste eines Eigentumsobjekts können zumindest Indiz für eine Rechtsgutbeeinträchtigung sein."[988]

- Schließlich könnte ein Substanzeingriff – in Parallele zum Eigentumsschutz gegen übermäßigen Steuerzugriff[989] – vorliegen, wenn eine Gesetzesänderung auf ein bereits bestehendes Unternehmen erdrosselnd oder konfiskatorisch wirkt (Erdrosselungskriterium). Die Widersprüchlichkeit dieser Erdrosselungsrechtsprechung des BVerfG wurde in der Literatur bereits gezeigt:[990] Danach schützt Art. 14 I S. 1 GG das Vermögen als solches nicht;[991] ist die Einwirkung auf das Vermögen hinreichend gewichtig („Erdrosselung") soll aber die Eigentumsgarantie betroffen sein.[992]

Im Ergebnis zeigen alle drei möglichen Kriterien zur Abgrenzung von nicht geschützter rechtlicher Rahmenbedingung zu eigentumsrechtlichem Substanzeingriff, dass es sich letztlich allein um eine Wertungsfrage handelt, wie auch immer dieses Bewertungskriterium benannt wird: Letztlich herrscht Einigkeit, dass *grundsätzlich* der Wegfall einer günstigen Gesetzeslage keine eigentumsrechtliche Relevanz hat, mithin nicht durch Art. 14 I S. 1 GG geschützte rechtliche Rahmenbedingung ist. *Ist die Veränderung aber derart gewichtig, dass bei wertender Betrachtung nicht nur zukünftige Erwerbschancen tangiert sind, sondern der eigentumsrechtlich geschützte Bestand so entwertet wird, dass vom Eigentumsrecht quasi nichts mehr übrig bleibt,*

987 *Stüer/Loges,* NVwZ 2000, 9, 13.
988 *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn. 24.
989 Vgl. dazu *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 160 ff., insbes. 163, 164.
990 *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 163.
991 Vgl. dazu *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 165 f., 169, der auch darlegt, weshalb eine Erstreckung des Grundrechtsschutzes der Eigentumsgarantie auf das Vermögen abzulehnen ist; *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn. 23.
992 *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 163: „Entweder berühren Abgabengesetze die Eigentumsgarantie, dann können sie unter bestimmten Umständen auch übermäßig belastend wirken; oder sie berühren sie nicht, dann bleiben sie eigentumsgrundrechtlich auch dann irrelevant, wenn sie im Einzelfall oder generell konfiskatorisch wirken."

ist dies als Eingriff in die Substanz des Eigentums und mithin als Eingriff in Art. 14 I S. 1 GG anzusehen. Ein klares Abgrenzungskriterium existiert nicht; vielmehr handelt es sich um eine einzelfallbezogene Wertungsfrage, bei der insbesondere auch Vertrauensschutzgesichtspunkte eine Rolle spielen:

> „Während der Bürger sich normalerweise nicht auf den Bestand von Gesetzen verlassen kann, darf er grundsätzlich auf den Fortbestand gesetzmäßig erworbener vermögenswerter Rechte vertrauen."[993]

cc) Absolutes Verschlüsselungsverbot als Substanzeingriff?

Hinsichtlich der Auswirkungen eines absoluten Verschlüsselungsverbotsgesetzes auf Hersteller und Anbieter von Verschlüsselungsprodukten ist folglich zu unterscheiden:

- Bietet ein Unternehmen etwa IT-Sicherheitslösungen – nach der Natur der Sache unter Verwendung von Verschlüsselungsverfahren – an, liegt *regelmäßig kein Substanzeingriff* vor. Der Bestand des Unternehmens bzw. seiner Bestandteile ist nicht gefährdet. Das Geschäftsfeld „IT-Sicherheit" besteht weiterhin fort, es muss jetzt nur ohne Verschlüsselungsverfahren auskommen. Dies mag zunächst zu (unter Umständen enormen) Umsatzeinbußen führen, da effektive IT-Sicherheitsverfahren ohne Verschlüsselung derzeit schwer vorstellbar sind; auch schwerwiegende Umsatzeinbußen reichen aber nicht für die Annahme eines Substanzeingriffs, wie die Entscheidung des BVerfG zu den Nichtraucherschutzgesetzen gerade wieder gezeigt hat.[994] Soweit einzelne Produkte oder Lösungen rechtlich geschütztes geistiges Eigentum darstellen, ist der Schutzbereich der Eigentumsgarantie natürlich eröffnet (s.o.). Auch für unternehmerisches Wissen in Form von Betriebs- und Geschäftsgeheimnissen ist der Schutzbereich eröffnet. Das wirtschaftliche Unternehmen und seine Bestandteile sind aber nicht in ihrer Substanz betroffen, so dass der Schutzbereich von Art. 14 I S. 1 GG insoweit nicht eröffnet ist.[995]
- Denkbar wäre die *Annahme eines Substanzeingriffs*, wenn ein Unternehmen nur *Produkte herstellt, die ohne Verschlüsselungsverfahren nicht existieren können*. Dann wäre – je nach Einzelfall – nicht nur das eventuell daran bestehende geis-

993 *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn. 64.

994 Siehe BVerfG, Urteil vom 30.07.2008, Az.: 1 BvR 3262/07 et al., Rn. 118, worin ausdrücklich auf die Umsatzrückgänge, die nach dem BVerfG „sogar zur Schließung des Geschäftsbetriebs zwingen" können, eingegangen wird; gleichwohl prüft das BVerfG eine Eröffnung des Geltungsbereichs von Art. 14 I S. 1 GG unter diesem Gesichtspunkt nicht mal, vgl. Rn. 91.

995 Parallel ist ein reines Exportverbot für Verschlüsselungsverfahren zu bewerten, wie es etwa mit Kategorie 5A2 des Anhang I der Verordnung 1334/2000 (EG) des Rates vom 22. Juni 2000 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr von Gütern und Technologien mit doppeltem Verwendungszweck (ABl. L 159 vom 30.6.2000, S. 1), geändert durch Verordnung 1183/2007 (EG) des Rates vom 18. September 2007 (ABl. L 278 vom 22.10.2007, S. 1) für starke Verschlüsselungsverfahren besteht.

tige Eigentumsrecht betroffen, sondern auch das Eigentum an weiteren das Unternehmen konstituierenden Rechtspositionen wäre entwertet. Die Rechtsposition „geistiges Eigentum an Verschlüsselungstechnologien“ würde für die Zukunft aus der Rechtsordnung eliminiert.[996] Das darauf basierende wirtschaftliche Unternehmen könnte nicht nur nicht weitergeführt werden (was ja Thema von Art. 12 I GG wäre), sondern wäre bereits aktuell in seinem Bestand entwertet: es kann für die Zukunft nicht genutzt werden, die neben dem Nutzungsrecht verbleibende Verfügungsbefugnis kann nicht wirtschaftlich sinnvoll realisiert werden.[997] In einem solchen Extremfall wäre nach allen oben dargestellten Meinungen der Schutzbereich von Art. 14 I S. 1 GG wegen eines Substanzeingriffs eröffnet.

- Auch hinsichtlich der *E-Commerce-Anbieter* geht es vor allem um die Tatsachenfrage, welche Auswirkungen ein absolutes Verschlüsselungsverbotsgesetz auf das Geschäftsmodell hätte. Einerseits könnte man vertreten, dass mit einem absoluten Verschlüsselungsverbot das gesamte Geschäftsmodell „Vertrieb von Waren via Internet“ zunichte gemacht würde, da dieser Geschäftszweig ganz maßgeblich von der (IT-)Sicherheit hinsichtlich Kundendaten, Bestellvorgängen, Bank- und Kreditkartendaten etc. abhinge. Da IT-Sicherheit derzeit maßgeblich auf Verschlüsselungsverfahren basiert, wären sichere E-Commerce-Verfahren ohne Verschlüsselung nicht denkbar. Voraussetzung dieser Auffassung wäre die Prognose, dass ohne sichere E-Commerce-Verfahren der elektronische Handel mangels Kundeninteresse (fast) gänzlich zum Erliegen käme, denn nur dann käme das für einen Substanzeingriff streitende Entwertungsargument zum Tragen.
  Da aber selbst massive Umsatzrückgänge allein nicht zu einem Substanzeingriff führen, könnte man andererseits vertreten, dass ein Verschlüsselungsverbot die E-Commerce-Anbieter nur zur Umgestaltung ihres Geschäftsmodells zwingen, dieses aber nicht ruinieren würde. Diese Umgestaltung mag zu nachlassender Bequemlichkeit des Online-Vertriebs führen, da etwa ein Online-Bestellvorgang allein nicht mehr hinreichend sicher wäre und daher zusätzlicher Maßnahmen bedarf, und in der Konsequenz zu zurückgehendem Kundeninteresse. Die Entwertungsgrenze wäre dabei aber nicht erreicht. Im Bereich des E-Commerce liegt daher regelmäßig kein Substanzeingriff durch ein absolutes Verschlüsselungsverbot vor.

996 Vgl. zur Beseitigung eines Segments der bisherigen Eigentumsordnung *Koch/Roßnagel,* NVwZ 2000, 1, 2 und 5.

997 Dies wäre natürlich Frage des konkreten Einzelfalls, ob eine Veräußerung geistiger Eigentumsrechte usw. – etwa ins Ausland – wirtschaftlich sinnvoll erfolgen könnte.

d. Zusammenfassung

Der Schutzbereich der Eigentumsfreiheit (Art. 14 I S. 1 GG) ist zum einen für Immaterialgüterrechte an oder unter Verwendung von Verschlüsselungsverfahren eröffnet (originärer Schutz von Verschlüsselung). Ebenfalls vom Schutzbereich erfasst sind Verschlüsselungsverfahren, die Betriebs- und Geschäftsgeheimnisse darstellen (originärer Schutz von Verschlüsselung). Verschlüsselungsverfahren sind weiter auch unter dem Aspekt des Schutzes von Eigentumspositionen (Immaterialgüterrechte oder Betriebs- und Geschäftsgeheimnisse) *durch* Verschlüsselung durch die Eigentumsgarantie geschützt (derivativer Schutz von Verschlüsselung). Jenseits dieses besonderen Geheimnisschutzes wird aber regelmäßig die wirtschaftliche Betätigung als Hersteller und Händler von Verschlüsselungsprodukten wie als E-Commerce-Anbieter nicht durch die Eigentumsgarantie geschützt. Nur ausnahmsweise kann in Einzelfällen die Auswirkung eines Verschlüsselungsverbots auf ein Geschäftsmodell derart gravierend sein, dass wegen eines Substanzeingriffs in den Eigentumsbestand doch Art. 14 I S. 1 GG einschlägig ist (derivativer Schutz von Verschlüsselung).

2. Grundrechtseingriff durch ein absolutes Verschlüsselungsverbot

Ein absolutes Verschlüsselungsverbotsgesetz könnte daher einen Eingriff in das durch Art. 14 I S. 1 GG geschützte Eigentum darstellen: Insoweit ist zwischen Inhalts- und Schrankenbestimmung (Art. 14 I S. 2 GG) einerseits und Enteignung (Art. 14 III GG) andererseits zu unterscheiden.

a. Inhalts- und Schrankenbestimmung (Art. 14 I S. 2 GG) oder Enteignung (Art. 14 III)?

Nach Art. 14 I S. 2 GG bestimmt der Gesetzgeber Inhalt und Schranken des Eigentums. Daher stellt eine Inhalts- und Schrankenbestimmung in diesem Sinne bei genauer Betrachtung gar keinen Eingriff in das grundrechtlich geschützte Eigentum dar, sondern konstituiert es erst.[998] Im Hinblick etwa auf die Institutsgarantie des Art. 14 I GG oder den Verhältnismäßigkeitsgrundsatz kann sich aber auch eine Inhalts- und Schrankenbestimmung als rechtswidrig darstellen, woraus sich dann doch ein Grundrechtseingriff ergeben würde. Schließlich ist die Inhalts- und Schrankenbestimmung von der Enteignung, die zweifelsohne einen klassischen Grundrechts-

998 So auch *Wieland*, in: *Dreier,* GG, Art. 14, Rn. 74.

eingriff darstellt, abzugrenzen,[999] so dass sich auch daher die Erörterung der Inhalts- und Schrankenbestimmung unter dem Punkt „Grundrechtseingriff“ rechtfertigt.

Das BVerfG definiert Inhalts- und Schrankenbestimmungen dabei wie folgt:

> „Solche Normen legen generell und abstrakt die Rechte und Pflichten des Eigentümers fest, bestimmen also den "Inhalt" des Eigentums. Der Gesetzgeber schafft damit auf der Ebene des objektiven Rechts diejenigen Rechtssätze, die die Rechtsstellung des Eigentümers begründen und ausformen; sie können privatrechtlicher und öffentlich-rechtlicher Natur sein.“[1000]

Diese Normen sind von der Legal- und der Administrativenteignung abzugrenzen:[1001]

> „Sie [die Enteignung; d. Verf.] ist auf die vollständige oder teilweise Entziehung konkreter subjektiver, durch Art. 14 Abs. 1 Satz 1 GG gewährleisteter Rechtspositionen zur Erfüllung bestimmter öffentlicher Aufgaben gerichtet. Die Enteignung setzt den Entzug konkreter Rechtspositionen voraus, aber nicht jeder Entzug ist eine Enteignung im Sinne von Art. 14 Abs. 3 GG. Diese ist beschränkt auf solche Fälle, in denen Güter hoheitlich beschafft werden, mit denen ein konkretes, der Erfüllung öffentlicher Aufgaben dienendes Vorhaben durchgeführt werden soll.“[1002]

aa) Enteignung (Art. 14 III GG)

Eine Enteignung ist somit nach Auffassung des BVerfG und weiten Teilen der Literatur[1003] durch folgende vier Merkmale gekennzeichnet:

- Entzug einer eigentumsrechtlichen Rechtsposition
- zur hoheitlichen Beschaffung von Gütern
- durch gezielten hoheitlichen Rechtsakt
- zur Erfüllung bestimmter öffentlicher Aufgaben[1004]

Danach wäre ein absolutes Verschlüsselungsverbot nicht als Enteignung anzusehen:

999 Vgl. zum Verhältnis von Inhalts- und Schrankenbestimmung zu Enteignung *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn. 52.

1000 BVerfGE 58, 300, 330 – Naßauskiesung.

1001 Vgl. zu den Begriffen der Legal- und Administrativenteignung BVerfGE 58, 300, 330 f. – Naßauskiesung: „Weiter hat der Gesetzgeber nach Art. 14 Abs. 3 Satz 2 GG die Möglichkeit, durch Gesetz einem bestimmten oder bestimmbaren Personenkreis konkrete Eigentumsrechte zu entziehen, die aufgrund der allgemein geltenden Gesetze im Sinne des Art. 14 Abs. 1 Satz 2 GG rechtmäßig erworben worden sind (Legalenteignung). Schließlich kann der Gesetzgeber – ebenfalls nach Art. 14 Abs. 3 Satz 2 GG – der Exekutive die Ermächtigung erteilen, konkretes Eigentum Einzelner zu entziehen. Die Enteignung aufgrund Gesetzes (Administrativenteignung) erfordert einen behördlichen Vollzugsakt, der – anders als die Legalenteignung – mit Rechtsmitteln angefochten werden kann.“

1002 BVerfG, Beschluss vom 22.05.2001, Az.: 1 BvR 1512/97 und 1677/97, Rn. 30.

1003 So *Wieland*, in: *Dreier,* GG, Art. 14, Rn. 78 m.w.N.

1004 Aufzählung nach *Wieland*, in: *Dreier,* GG, Art. 14, Rn. 77; im Ergebnis inhaltsgleich auch *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn. 58 sowie *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 204.

- Es fehlt an einer *hoheitlichen Güterbeschaffung zur Erfüllung öffentlicher Aufgaben*. Ein absolutes Verschlüsselungsverbot dient nicht dazu, bestimmte Verschlüsselungsverfahren dem Staat zugänglich zu machen, um damit ein konkretes Vorhaben durchzuführen. Der Staat, insbesondere Militär und Geheimdienst verfügen bereits über hocheffektive Verschlüsselungstechnologien. Ein Verschlüsselungsverbotsgesetz soll nur verhindern, dass auch Private effektiv verschlüsseln können. Diese Zielsetzung dient zwar ebenfalls der Erfüllung öffentlicher Aufgaben (Prävention und Verfolgung von Straftaten), aber nur mittelbar im Wege der Verhinderung der Nutzung von Technologien, die im Einzelfall Prävention und Verfolgung von Straftaten erschweren könnten. Der Staat beschafft sich also gerade nicht selbst Verschlüsselungstechnologien, um diese zu nutzen, er verhindert nur die Nutzung solcher Technologien durch den Einzelnen. Darin liegt kein Güterbeschaffungsvorgang.
- Auch ist zweifelhaft, ob man von einem *gezielten hoheitlichen Rechtsakt* sprechen kann. Primärziel eines Verschlüsselungsverbotsgesetzes ist die Untersagung der Nutzung von Verschlüsselungstechnologien, um staatliche Überwachungsoptionen zu erhalten. Daraus ergibt sich eine Betroffenheit der Inhaber von Rechtspositionen nach Art. 14 I S. 1 GG, seien es Inhaber von Immaterialgüterrechten an Verschlüsselungsverfahren oder Inhaber von Betriebs- und Geschäftsgeheimnissen oder sonstigem unternehmerischen Know-how. Ein Verschlüsselungsverbot hat aber nicht das Ziel, diese Rechtspositionen zu entziehen.[1005] [1006]
- Schließlich ist zwar der *Entzug einer eigentumsrechtlich geschützten Rechtsposition* Voraussetzung der Enteignung, doch nicht jeder Entzug einer solchen Rechtsposition stellt auch eine Enteignung dar. Auch Inhalts- und Schrankenbestimmungen können zur Entziehung von Rechtpositionen führen, insbesondere bei der gesetzgeberischen Umgestaltung von eigentumsrechtlichen Regelungen:[1007]

  „[…]; die Eigentumsgarantie gebietet insoweit nicht, einmal ausgestaltete Rechtspositionen für alle Zukunft in ihrem Inhalt unangetastet zu lassen. Selbst die völlige Beseitigung bisher bestehender, durch die Eigentumsgarantie geschützter Rechtspositionen kann unter bestimmten Voraussetzungen zulässig sein.“[1008]

1005 Vgl. insbesondere *Koch/Roßnagel,* NVwZ 2000, 1, 2 mit vielen weiteren Nachweisen zur entsprechenden Debatte für den Atomausstieg: Während die einen als alleinigen Zweck eines „Ausstiegsgesetzes“ die Beseitigung des Eigentums an bestehenden Kernkraftanlagen ansehen, vertreten die anderen, dass Primärziel eines solchen Gesetzes das Verbot einer bestimmten Form der Stromerzeugung aufgrund veränderter Risikobewertung sei.

1006 Anders könnte dies zu bewerten sein, falls mit der Voraussetzung des gezielten Hoheitsakts lediglich „Zufallsenteignungen“ ausgeschlossen werden sollen, wie dies *Wieland*, in: *Dreier,* GG, Art. 14, Rn. 78 zu vertreten scheint.

1007 So *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn. 57.

1008 BVerfGE 83, 201, 212.

Andersfalls könnten Inhalt und Schranken eigentumsrechtlicher Regelungen niemals durch den Gesetzgeber verändert werden, da jede Minderung von Eigentümerrechten

„am Tag ihres Inkrafttretens einen an diesem Stichtag bestimmbaren Kreis von Eigentümern in seinen auf der Grundlage alten Rechts erworbenen Rechten [trifft; d. Verf.].“[1009]

Daraus folgt, dass der Entzug eigentumsrechtlich geschützter Rechtspositionen auch im Wege der gesetzgeberischen Um- oder Neugestaltung eines Rechtsgebiets, mithin der Inhalts- und Schrankenbestimmung, erfolgen kann:

„Die gesetzliche Beseitigung eines nach Art. 14 Abs. 1 Satz 1 GG geschützten Rechts ist nicht in jedem Falle eine (Legal-)Enteignung. […] Der Gesetzgeber darf nicht nur nach Art. 14 Abs. 1 Satz 2 GG Eigentumsrechten einen neuen Inhalt geben. Ebenso wie er neue Rechte einführen darf, kann er auch das Entstehen von Rechten, die nach bisherigem Recht möglich waren, für die Zukunft ausschließen. Es ist ihm auch nicht ausnahmslos verwehrt, die nach altem Recht begründeten Rechte der Neuregelung anzugleichen, selbst wenn dabei die bisher mit dem Recht verbundenen Befugnisse eingeschränkt werden; […].“[1010]

So liegt es auch bei einem absoluten Verschlüsselungsverbot. Das Gebiet „nicht-staatliche Nutzung von Verschlüsselungsverfahren“ wird neu geregelt. Dadurch werden zum Teil nach bisherigem Recht existierende Rechte beseitigt. Unmittelbar werden etwa die Nutzungsrechte hinsichtlich geistigen Eigentums beschränkt, da in Deutschland Verschlüsselungstechnologien nicht mehr verwendet werden dürften. Mittelbar werden dadurch natürlich auch weitere Verwertungsmöglichkeiten eingeschränkt oder sogar de facto beseitigt, etwa die Veräußerungsrechte. Insoweit scheint vertretbar, von einer Beseitigung des geistigen Eigentums an Verschlüsselungsverfahren zu sprechen mit dem Argument, dass eine wirtschaftlich sinnvolle Nutzung nicht mehr möglich sei. Inwieweit eine Nutzung im oder eine Veräußerung ins Ausland tatsächlich möglich sind, wäre insofern klärungsbedürftig. Für die Abgrenzung von Enteignung und Inhalts- und Schrankenbestimmung kommt es darauf aber nicht an. Entscheidend ist vielmehr, dass die Eigentumsordnung generell hinsichtlich Verschlüsselungstechnologien geändert wird und deswegen bestimmte Eigentumspositionen an sich beseitigt werden; demgegenüber wäre Kennzeichen einer Enteignung, dass das Eigentumsrecht an sich fortbesteht und nur manchen Eigentümern ihr konkretes Eigentum entzogen wird:

„Diese substanzielle Rechtfertigung liegt darin, dass in den als Enteignung einzuordnenden Fällen die Eigentumsordnung aufrecht erhalten wird und lediglich einige ihr Eigentum zu Gunsten öffentlicher Interessen aufgeben müssen, während die Fälle der Entziehung alter Rechte bei Gelegenheit der Eigentumsinhaltsneubestimmung dadurch gekennzeichnet sind, dass die Gesellschaft bestimmte Eigentumspositionen als mit wichtigen Allgemeinwohlbelangen nicht mehr vereinbar ansieht und daher generell beseitigt.“[1011]

1009 *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn. 56.
1010 BVerfGE 83, 201, 211 f.
1011 *Koch/Roßnagel,* NVwZ 2000, 1, 6.

bb) Inhalts- und Schrankenbestimmung (Art. 14 I S. 2 GG)

Folglich würde ein absolutes Verschlüsselungsverbotsgesetz keine Enteignung (Art. 14 III GG) darstellen, sondern eine Inhalts- und Schrankenbestimmung (Art. 14 I S. 2 GG). Dies gilt auch für einen eigentumsrechtlichen Schutz von Verschlüsselungsverfahren als Mittel zum Schutz von Betriebs- und Geschäftsgeheimnissen (derivativer Schutz von Verschlüsselungsverfahren). Auch hier fehlt es bereits an einem gezielten hoheitlichen Rechtsakt und einem hoheitlichen Güterbeschaffungsvorgang. Schließlich ist fraglich, ob durch das Verbot *eines* Mittels zum Schutz von Betriebs- und Geschäftsgeheimnissen eine Rechtsposition entzogen wird. Für die Annahme einer Entziehung von Rechtspositionen spricht das exorbitante Gefährdungspotential von Industrie- und Wirtschaftsspionage, dem nur mit Mitteln der IT-Sicherheit, folglich unter Einsatz von Verschlüsselungsverfahren, begegnet werden kann. Daher könnte man argumentieren, dass ohne die Möglichkeit eines derartigen Schutzkonzepts die Betriebs- und Geschäftsgeheimnisse Spionageversuchen de facto schutzlos ausgeliefert wären, so dass die formell bestehende Rechtsposition tatsächlich entwertet ist. Gegen die Annahme einer Entziehung von Rechtspositionen könnte dagegen vorgebracht werden, dass Betriebs- und Geschäftsgeheimnisse weiterhin etwa durch strafrechtliche Normen geschützt sind, so dass von einer völligen Preisgabe von Betriebs- und Geschäftsgeheimnissen nicht gesprochen werden kann. Festzuhalten bleibt, dass ein absolutes Verschlüsselungsverbot in jedem Fall eine Inhalts- und Schrankenbestimmung und keine Enteignung darstellen würde.[1012]

b. Verfassungsmäßigkeit der Inhalts- und Schrankenbestimmung

Diese Inhalts- und Schrankenbestimmung müsste verfassungsgemäß sein, das heißt insbesondere dem Abwägungsgebot (zwischen der Eigentumsgewährleistung einerseits und der Allgemeinwohlbezogenheit andererseits), dem Gleichheitssatz, dem Verhältnismäßigkeitsprinzip und dem Vertrauensschutzgedanken genügen.[1013] Andernfalls schlägt die Inhalts- und Schrankenbestimmung nicht in eine Enteignung um, sondern ist schlicht verfassungswidrig.[1014]

Erste Voraussetzung wäre allerdings die Verfassungsmäßigkeit der Eigentumsinhaltsneubestimmung als solcher:[1015]

> „Voraussetzung der Zulässigkeit eines Eingriffs in bestehende Rechtspositionen durch eine gesetzliche Neuregelung ist zunächst, daß die Neuregelung als solche, unabhängig von der Frage der Beseitigung oder Einschränkung bestehender Rechtspositionen, verfassungsmäßig ist.“[1016]

1012 So für den Atomausstieg auch *Stoll*, Sicherheit als Aufgabe von Staat und Gesellschaft, S. 180 ff., der sich auch umfassend mit Gegenargumenten auseinandersetzt.

1013 *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn.

1014 *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 203; *Stoll*, Sicherheit als Aufgabe von Staat und Gesellschaft, S. 180.

1015 *Koch/Roßnagel,* NVwZ 2000, 1, 5.

Daran würde es aber bereits fehlen, da ein absolutes Verschlüsselungsverbotsgesetz gegen Grundrechte (etwa Fernmeldegeheimnis, Art. 10 I GG, und allgemeines Persönlichkeitsrecht, Art. 2 I GG i.V.m. Art. 1 I GG) verstoßen würde.

aa) Abwägungsgebot

Art. 14 II GG enthält Leitlinien für den Gesetzgeber zur verfassungsgerechten Eigentumsausgestaltung; das konkrete Verhältnis von privat- und fremdnützigem Eigentumsgebrauch bestimmt der Gesetzgeber.[1017] Dazu gehört unter Umständen auch die Schaffung von Entschädigungsregelungen.[1018] Allerdings kann auch eine Ausgleichregelung aus einer generell unverhältnismäßigen Inhalts- und Schrankenbestimmung keine verhältnismäßige machen.[1019] Entscheidend ist die Abwägung mit den Allgemeinwohlbelangen:

> „Der Gesetzgeber muß bei der Bestimmung von Inhalt und Schranken des Eigentums im Sinne von Art. 14 Abs. 1 Satz 2 GG die schutzwürdigen Interessen des Eigentümers und die Belange des Gemeinwohls in einen gerechten Ausgleich und ein ausgewogenes Verhältnis bringen. Er muß sich dabei im Einklang mit allen anderen Verfassungsnormen halten; insbesondere ist er an den verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit und den Gleichheitssatz des Art. 3 Abs. 1 GG gebunden. Das Wohl der Allgemeinheit ist nicht nur Grund, sondern auch Grenze für die dem Eigentum aufzuerlegenden Belastungen.“[1020]

Die im Wege eines absoluten Verschlüsselungsverbots verfolgten Allgemeinwohlbelange sind Prävention und Verfolgung von Straftaten sowie die Sicherung des Rechtsfriedens. Diesen überragend wichtigen Gemeinwohlinteressen stehen zum einen die nach altem Recht wohlerworbenen Rechte (Immaterialgüterrechte oder Betriebs- und Geschäftsgeheimnisse) gegenüber. Zum anderen ist bei der Eigentumsinhaltsneubestimmung für die Zukunft ebenfalls eine Balance von Eigen- und Fremdnützigkeit zu finden, wenn auch eine größere politische Gestaltungsfreiheit des Gesetzgebers herrschen dürfte, da Vertrauensschutzgesichtspunkte eine geringere Rolle

1016 BVerfGE 83, 201, 212.

1017 *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 218.

1018 BVerfGE 83, 201, 212, 213: „Selbst wenn Art. 14 Abs. 3 GG nicht unmittelbar eingreift, ist das darin zum Ausdruck kommende Gewicht des Eigentumsschutzes bei der vorzunehmenden Abwägung zu beachten, da sich der Eingriff für den Betroffenen wie eine (Teil- oder Voll-)Enteignung auswirkt. Der Gesetzgeber muß danach die Umgestaltung oder Beseitigung eines Rechts zwar nicht durchweg mit einer Entschädigungs- oder Übergangsregelung abmildern. Die völlige, übergangs- und ersatzlose Beseitigung einer Rechtsposition kann jedoch nur unter besonderen Voraussetzungen in Betracht kommen.“

1019 *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 236: „Diese [die Inhalts- und Schrankenbestimmungen; d. Verf.] müssen vielmehr grundsätzlich auch ohne Ausgleichregelungen die Substanz des Eigentums wahren und dem Gleichheitsgebot entsprechen; sie sind dann vom Eigentümer grundsätzlich entschädigungslos hinzunehmen. Nur wenn die Anwendung des Gesetzes im Einzelfall zu einer unzumutbaren Belastung führt, können gesetzliche Ausgleichsregelungen in Betracht kommen.“

1020 BVerfG, Beschluss vom 02.03.1999, Az.: 1 BvL 7/91, Rn. 83.

spielen.[1021] Zuletzt sind die Geheimnisschutzinteressen der Inhaber von Betriebs- und Geschäftsgeheimnissen zu berücksichtigen, die – unabhängig vom Inhalt des Betriebs- oder Geschäftsgeheimnisses – bei der Nutzung von IT ihre Geheimnisse nicht wirkungsvoll gegen Konkurrenzausspähung und Wirtschaftsspionage sichern können.

bb) Verhältnismäßigkeitsprinzip

Diese Abwägungsentscheidung des Gesetzgebers zwischen Privatnützigkeit und Sozialpflichtigkeit ist insbesondere am Verhältnismäßigkeitsgrundsatz zu messen.[1022] Danach wäre eine Eigentumsinhaltsneubestimmung dergestalt, dass das Entstehen eigentumsrechtlicher Rechtspositionen an Verschlüsselungsverfahren ausgeschlossen wird, wegen des Gewichts der zu schützenden Allgemeinwohlinteressen wohl zu rechtfertigen. Da für die Zukunft bereits die Arbeit an und mit Verschlüsselungsverfahren in Deutschland nicht mehr legal möglich wäre, würde dieser Wirtschaftssektor schlicht aussterben. Gegebenenfalls entstehende besondere Härten könnten durch Ausgleichsregelungen abgemildert werden.

Auch im Hinblick auf die nach alter Rechtslage bereits erworbenen Rechte hinsichtlich Verschlüsselungsverfahren könnte man noch vertreten, dass eine verhältnismäßige Abwägungsentscheidung möglich sei. Großzügige Entschädigungsregelungen könnten angesichts des hohen Rangs der involvierten Allgemeinwohlinteressen dem Vertrauensschutzgedanken Rechnung tragen. Überleitungsvorschriften dürften dagegen im konkreten Fall weniger in Betracht kommen, da der Gesetzgeber im Kern die möglichst umfassende Tilgung von Verschlüsselungsverfahren anstrebt. Würde er aus Vertrauensschutzgesichtspunkten für eine Übergangszeit etwa den Export von Verschlüsselungsprodukten noch gestatten, könnte dies auch als Konterkarierung des Zwecks eines Verschlüsselungsverbots angesehen werden: Da Verschlüsselungsverfahren insbesondere auch heimlich verwendet werden können, würde jedes weitere legale Vorhandensein von Verschlüsselungsverfahren es weiter erschweren, solche Umgehungsmaßnahmen zu verhindern. Und eine solche Einschätzung könnte die Geeignetheit eines Verschlüsselungsverbots weiter unterminieren.

Jedenfalls kann ein absolutes Verschlüsselungsverbotsgesetz mit Blick auf den Schutz von Betriebs- und Geschäftsgeheimnissen in keinem Fall verhältnismäßig sein. Ähnlich wie bereits im Rahmen des grundrechtlichen Privatsphärenschutzes steht den Allgemeinwohlinteressen eine breite Betroffenheit in vitalen wirtschaftlichen Interessen gegenüber, deren Schutz der Staat mittels der ihm zur Verfügung stehenden Mechanismen nicht gewährleisten kann. Ein Verzicht auf IT durch die Unternehmer stellt angesichts des internationalen Wettbewerbs keine Option dar. Ein Großteil der Unternehmen würde somit gegenüber Konkurrenzausspähung und

1021 *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 225.
1022 *Bryde*, in: *v. Münch/Kunig,* GG, Art. 14, Rn. 63.

Wirtschaftsspionage schutzlos gestellt, da eine zentrale Maßnahme zum Schutz von Betriebs- und Geschäftsgeheimnissen untersagt würde. Andere Schutzmaßnahmen blieben zwar möglich, ließen sich aber nicht technisch absichern und abbilden. Was würde es beispielweise nutzen, seine Mitarbeiter dafür zu sensibilisieren, keine wichtigen Unterlagen offen in den Betriebsräumen herumliegen zu lassen, wenn gleichzeitig keinerlei Zugangshindernisse hinsichtlich der Rechner bestehen? Ein absolutes Verschlüsselungsverbot bedeutet die rechtliche Preisgabe jeglicher Betriebs- und Geschäftsgeheimnisse. Dies kann auch mit noch so gewichtigen Allgemeinwohlinteressen nicht gerechtfertigt werden. Die Bedenken hinsichtlich der Geeignetheit eines Verschlüsselungsverbotsgesetzes gelten hier gleichermaßen.

3. Ergebnis

Daher würde im Ergebnis ein absolutes Verschlüsselungsverbotsgesetz einen Verstoß gegen Art. 14 I S. 1 GG darstellen, da ein derartiges Verbot keine verfassungsmäßige Inhalts- und Schrankenbestimmung darstellen kann.

II. Verstoß gegen die Berufsfreiheit (Art. 12 I GG)

Ein absolutes Verschlüsselungsverbotsgesetz könnte daneben auch gegen die Berufsfreiheit (Art. 12 I GG) verstoßen:

- Ein solcher Verstoß kommt zunächst wegen des mit einem Verschlüsselungsverbot einhergehenden Verbots des Besitzes, der Verwendung, der Herstellung und des Vertriebs von Verschlüsselungsprodukten in Betracht (*originärer Schutz* von Verschlüsselung).
- Daneben könnte sich aber auch ein Eingriff in Berufsgeheimnisse ergeben – was sich nicht nur im Bereich der Berufsgeheimnisträger als Verstoß gegen die Berufsfreiheit erweisen könnte (*derivativer Schutz* von Verschlüsselung).

1. Schutzbereich der Berufsfreiheit (Art. 12 I GG)

Art. 12 I GG schützt die berufliche Tätigkeit, und zwar sowohl hinsichtlich der Berufsausübung als auch hinsichtlich der Berufswahl, da eine klare Grenzziehung zwischen den einzelnen Garantien nach Auffassung des BVerfG nicht möglich ist.[1023]

1023 Berufswahl und Berufsausübung bilden insoweit ein einheitliches Grundrecht der Berufsfreiheit: „Zwischen den einzelnen Garantien von Art. 12 Abs. 1 GG ist keine klare Grenzziehung möglich. Art. 12 Abs. 1 GG formuliert ein einheitliches Grundrecht der Berufsfreiheit, dessen verschiedene Gewährleistungen allerdings insofern Bedeutung haben, als an die Einschränkung von Berufs- und Arbeitsplatzwahl höhere Anforderungen gestellt werden als an die Einschränkung der Berufsausübung." (BVerfGE 92, 140, 151); so auch BVerfGE 95, 193, 214;

Beruf ist dabei jede „auf Dauer angelegte Tätigkeit zur Schaffung und Erhaltung einer Lebensgrundlage“, unabhängig davon, ob diese Tätigkeit freiberuflich, selbstständig oder unselbständig erfolgt.[1024]

a. Beruf und Berufsbild

Herstellung und Vertrieb von Verschlüsselungsprodukten stellen danach eindeutig einen Beruf im Sinne des Art. 12 I GG dar. Zu beantworten bleibt lediglich die Frage, ob es sich um ein eigenständiges Berufsbild handelt (mit der Folge, dass eine Untersagung der Tätigkeit eine Berufs*wahl*regelung wäre) oder ob es sich um eine unter mehreren möglichen Betätigungen innerhalb eines weiter gefassten Berufsbildes handelt (mit der Konsequenz, dass ein Verschlüsselungsverbot nur als Berufs*ausübung*sregelung anzusehen wäre).[1025] Es handelt sich wiederum um eine Frage des Einzelfalls:

- Der Unternehmer, der IT-Sicherheitsprodukte oder –dienste[1026] und/oder Verschlüsselungsprodukte vertreibt, ist jenseits der Frage, wie man sein Berufsbild einordnen würde, sicher nicht in seiner Berufswahlfreiheit betroffen; er kann seinen Beruf weiter ausüben, nur eben unter veränderten äußeren Bedingungen.[1027] Eventuell sich ergebende Absatzschwierigkeiten oder Umsatzrückgänge entfalten erst dann grundrechtliche Relevanz, wenn sie erdrosselnde Wirkung haben.[1028]

Mann, in: *Sachs*, GG, Art. 12, Rn. 14, 77; *Manssen*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 12, Rn. 2 f.; *Wieland*, in: *Dreier,* GG, Art. 12, Rn. 62.

1024 *Manssen*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 12, Rn. 36; *Wieland*, in: *Dreier,* GG, Art. 12, Rn. 49 ff.; *Gubelt*, in: *v. Münch/Kunig,* GG, Art. 12, Rn. 8.

1025 So auch *Stüer/Loges,* NVwZ 2000, 9, 11; *Manssen*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 12, Rn. 52.

1026 Dabei ist etwa an Anonymisierungsdiensteanbieter zu denken. *Möller,* DuD 2000, 267, 270 sieht ebenfalls den Schutzbereich der Berufsfreiheit eröffnet, äußert sich dann aber nicht speziell zur verfassungsrechtlichen Rechtfertigung.

1027 Anderer Ansicht insoweit *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 208, der ein Verbot des Herstellens und Anbietens von Verschlüsselungsverfahren wegen der Monopolisierung der Bereitstellung von Verschlüsselungsverfahren durch den staatlichen Geheimschutzsektor als Berufswahlregelung ansieht. Zwar werden solche Monopole der öffentlichen Hand vielfach als objektive Zulassungsschranken angesehen (vgl. insoweit nur *Wieland*, in: *Dreier,* GG, Art. 12, Rn. 79 f.), hier liegt in Wirklichkeit jedoch keine Monopolbildung vor. Ein absolutes Verschlüsselungsverbot bedeutet nicht das Verbot an Private, Verschlüsselungsverfahren herzustellen und zu vertreiben bei gleichzeitiger Erlaubnisvergabe an staatliche Stellen, dies zu tun. Ein absolutes Verschlüsselungsverbot beseitigt den Markt „Verschlüsselungsverfahren für den privaten Einsatz“ vollständig. Darin liegt nach hier vertretener Auffassung kein Monopol.

1028 So zumindest die Schwelle bei Steuern und Abgaben sowie staatlichen Wettbewerbsbeeinflussungen, vgl. *Wieland*, in: *Dreier,* GG, Art. 12, Rn. 86, 88. Für die hier angesprochene Unternehmerfreiheit kann nichts anderes gelten, worauf auch schon der enge Zusammenhang mit der Eigentumsfreiheit nach Art. 14 I S. 1 GG hinweist. Geschützt wird nur die grundsätz-

„Die Freiheit der Berufswahl könnte daher nur dann beeinträchtigt sein, wenn das Verbot wegen seiner Auswirkungen die sinnvolle Ausübung dieses Berufs faktisch unmöglich machen würde."[1029]

- Aber auch bei einem hoch spezialisierten Kryptologen liegt in der Regel kein eigenständiges Berufsbild vor, es dürfte sich vielmehr um ein Teilgebiet der Mathematik und vor allem der Informatik handeln. Entscheidend für diese Ermittlung des Berufsfeldes sind – soweit es an einer Typisierung durch den Gesetzgeber fehlt – die rechtlichen und tatsächlichen, insbesondere sozialen und wirtschaftlichen Gegebenheiten unter Berücksichtigung der Anschauungen der Allgemeinheit, der Berufsausübenden selbst wie deren Vertragspartnern.[1030] Für den vorliegenden Bereich ist angesichts der universitären Ausbildung eine gewisse Typisierung anzutreffen, wonach die Kryptographie Teil der (theoretischen) Informatik ist (mit Schnittstellen zur Mathematik). Einen eigenständigen Ausbildungsberuf gibt es nicht, vielmehr dürfte kryptographisches Wissen in etlichen Berufen der Hard- und Softwareentwicklung gefordert sein.[1031] Das BVerfG[1032] hat etwa bei der Frage, ob eine Facharzttätigkeit im Verhältnis zur ärztlichen Berufsausübung ein eigenständiges Berufsbild darstelle, keine eindeutige Antwort finden können und in der Facharzttätigkeit Elemente erkannt, „die einer Berufswahl nahe kämen."[1033] Daraus würden sich eventuell höhere Anforderungen an die Allgemeinwohlerwägungen, die den Eingriff in die Berufsfreiheit legitimieren sollen, sowie an bei der Prüfung der Verhältnismäßigkeit anzuwendende Maßstäbe ergeben. Für die Mehrzahl der Betroffenen dürfte allerdings *nicht* das gesamte Berufsbild und damit die Berufs*ausübungs*freiheit betroffen sein.

liche Möglichkeit zu beruflichem Erwerb, die Chancen und Risiken unternehmerischer Tätigkeit hat der Unternehmer grundsätzlich selbst zu tragen; vgl. dazu ausführlich *Manssen*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 12, Rn. 68 ff.

1029 BVerfGE 61, 291, 309 – Tierpräparatoren – für umfassende Besitz-, Verarbeitungs- und Vertriebsverbote hinsichtlich bestimmter artengeschützter Tiere.

1030 *Gubelt*, in: *v. Münch/Kunig,* GG, Art. 12, Rn. 12; *Manssen*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 12, Rn. 52.

1031 Vgl. insoweit die Berufsfeld-Übersicht der Agentur für Arbeit unter http://berufenet.arbeitsagentur.de/berufe /themeSearch.do (27.08.2008), die einen umfassenden Überblick über einzelne Berufe gibt.

1032 Vgl. BVerfGE 33, 125, 161: „Es kann dahingestellt bleiben, ob der Facharzt im Sinne der Rechtsprechung des Bundesverfassungsgerichts zu Art. 12 Abs. 1 GG als ein besonderer Berufszweig innerhalb des allgemeinen Berufs "Arzt" angesehen werden könnte. Es lassen sich Gründe für diese Auffassung anführen. Doch selbst wenn man auch für den Bereich des Art. 12 GG an der Einheit des ärztlichen Berufs festhält, die Tätigkeit des Facharztes also nur als eine besondere Form der Berufsausübung innerhalb des einheitlichen Arztberufs ansieht, läßt sich nicht verkennen, daß der Entscheidung, sich dieser Tätigkeit zu widmen, Elemente innewohnen, die einer Berufswahl nahekommen."

1033 *Wieland*, in: *Dreier,* GG, Art. 12, Rn. 54 unter Verweis auf die soeben genannte BVerfG-Entscheidung.

b. Schutz des Berufsgeheimnisses?

Zu prüfen ist, ob Art. 12 I GG auch das Berufsgeheimnis schützt. Dies wird zum Teil in der Literatur behauptet – allerdings ohne nähere Begründung.[1034] Für einzelne Berufszweige ist das Berufsgeheimnis als integraler Bestandteil der Tätigkeit durch Rechtsprechung und Literatur anerkannt, etwa die durch Art. 5 I S. 2 GG gewährleistete Vertraulichkeit der Pressearbeit:[1035]

> „Die Pressefreiheit umfasst auch den Schutz vor dem Eindringen des Staates in die Vertraulichkeit der Redaktionsarbeit sowie in die Vertrauenssphäre zwischen den Medien und ihren Informanten. Die Freiheit der Medien ist konstituierend für die freiheitliche demokratische Grundordnung. Eine freie Presse und ein freier Rundfunk sind daher von besonderer Bedeutung für den freiheitlichen Staat. Dementsprechend gewährleistet Art. 5 Abs. 1 Satz 2 GG den im Bereich von Presse und Rundfunk tätigen Personen und Organisationen Freiheitsrechte und schützt darüber hinaus in seiner objektiv-rechtlichen Bedeutung auch die institutionelle Eigenständigkeit der Presse und des Rundfunks. Die Gewährleistungsbereiche der Presse- und Rundfunkfreiheit schließen diejenigen Voraussetzungen und Hilfstätigkeiten mit ein, ohne welche die Medien ihre Funktion nicht in angemessener Weise erfüllen können. Geschützt sind namentlich die Geheimhaltung der Informationsquellen und das Vertrauensverhältnis zwischen Presse beziehungsweise Rundfunk und den Informanten. Dieser Schutz ist unentbehrlich, weil die Presse auf private Mitteilungen nicht verzichten kann, diese Informationsquelle aber nur dann ergiebig fließt, wenn sich der Informant grundsätzlich auf die Wahrung des Redaktionsgeheimnisses verlassen kann.“[1036]

Gleiches gilt für das durch die Religionsfreiheit geschützte kirchenrechtliche Beichtgeheimnis.[1037] Das besondere Vertrauensverhältnis zwischen Rechtsanwalt (insbesondere in seiner Funktion als Strafverteidiger) und Mandant wird ebenfalls grundrechtlich geschützt, laut BVerfG durch das Recht auf ein rechtstaatlich faires Verfahren als Ausprägung der allgemeinen Handlungsfreiheit (Art. 2 I GG):[1038]

> „Von dem Datenzugriff ist auch das Recht auf ein rechtsstaatlich faires Verfahren gemäß Art. 2 Abs. 1 GG und das hieraus resultierende Recht auf eine vertrauliche Kommunikation zwischen dem Rechtsanwalt als Strafverteidiger und seinem Mandanten betroffen. Wie bei dem Eingriff in das Recht auf informationelle Selbstbestimmung hat das Bundesverfassungsgericht den Schutz der drittbetroffenen Mandanten vor einem übermäßigen Datenzugriff zu gewährleisten. Auch hier ist von Bedeutung, dass Mandanten nicht durch die Gefahr eines unbeschränkten Informationszugriffs der Strafverfolgungsbehörden an einer offenen, rückhaltlosen und vertrauensvollen Kommunikation mit ihren Verteidigern gehindert werden dürfen.“[1039]

1034 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 208; *Kloepfer,* Informationsrecht, § 3, Rn. 57; für das Bankgeheimnis *Groß,* KritJ 2002, 1, 7 f.

1035 Vgl. dazu *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 5, Rn. 62.

1036 BVerfG, Urteil vom 27.02.2007, Az.:1 BvR 538/06 und 2045/06, Rn. 41 f. – Cicero.

1037 *Kloepfer,* Informationsrecht, § 3, Rn. 57.

1038 Gegebenenfalls in Verbindung mit Art. 20 III, vgl. *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 128 ff.

1039 BVerfG, Beschluss vom 12.04.2005, Az.: 2 BvR 1027/02, Rn. 88.

Daneben betont das BVerfG aber auch den Zusammenhang von Vertrauensverhältnis und anwaltlicher Berufsausübung:[1040]

> „Voraussetzung für die Erfüllung dieser Aufgabe ist ein Vertrauensverhältnis zwischen Rechtsanwalt und Mandant. Integrität und Zuverlässigkeit des einzelnen Berufsangehörigen sowie das Recht und die Pflicht zur Verschwiegenheit sind die Grundbedingungen dafür, dass dieses Vertrauen entstehen kann. Die Verschwiegenheitspflicht rechnet daher von jeher zu den anwaltlichen Grundpflichten. Als unverzichtbare Bedingung der anwaltlichen Berufsausübung hat sie teil am Schutz des Art. 12 Abs. 1 Satz 1 GG."[1041]

Es scheint insoweit noch keine vollständige Klarheit über die Einordnung der nicht (wie im Falle von Redaktions- oder Beichtgeheimnis) spezialgrundrechtlich geschützten Berufsgeheimnisse zu herrschen. In einer späteren Entscheidung hat das BVerfG das Vertraulichkeitsverhältnis zwischen Rechtsanwalt und Mandant nicht mehr als in jedem Falle durch die Berufsfreiheit geschützt angesehen:

> „Dem Rechtsanwalt als berufenem unabhängigen Berater und Beistand obliegt es, im Rahmen seiner freien und von Art. 12 Abs. 1 Satz 1 GG geschützten Berufsausübung seinen Mandanten umfassend beizustehen. Voraussetzung für die Erfüllung dieser Aufgabe ist ein Vertrauensverhältnis zwischen Rechtsanwalt und Mandant. Von Bedeutung ist hierbei, dass das von dem Datenzugriff berührte Tätigwerden des Anwalts auch im Interesse der Allgemeinheit an einer wirksamen und geordneten Rechtspflege liegt. Das Bundesverfassungsgericht hat mehrfach die fundamentale objektive Bedeutung der "freien Advokatur" hervorgehoben. Diese objektiv-rechtliche Bedeutung der anwaltlichen Tätigkeit und des rechtlich geschützten Vertrauensverhältnisses zwischen Rechtsanwalt und Mandant wird jedenfalls dann berührt, wenn wegen der Gefahr eines unbeschränkten Datenzugriffs ein Mandatsverhältnis von Anfang an mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet wird. Mit dem Ausmaß potentieller Kenntnis staatlicher Organe von vertraulichen Äußerungen wächst die Gefahr, dass sich auch Unverdächtige nicht mehr den Berufsgeheimnisträgern zur Durchsetzung ihrer Interessen anvertrauen."[1042]

In derselben Entscheidung sieht das BVerfG zudem die wirtschaftliche Betätigungsfreiheit als Ausprägung der allgemeinen Handlungsfreiheit (Art. 2 I GG) dadurch betroffen, dass – im vorliegenden Fall durch den Zugriff auf den gesamten Datenbestand einer Rechtsanwaltskanzlei – das Vertrauensverhältnis Schaden nimmt und daraufhin das Mandatsverhältnis beendet wird:

> „Es besteht zudem die Gefahr, dass Mandanten, welchen der Zugriff der Strafverfolgungsbehörden auf auch sie betreffende und regelmäßig vertrauliche Daten bekannt wird, das Mandatsverhältnis zu ihrem Rechtsanwalt oder Steuerberater kündigen. Damit hat der Zugriff auf die Kanzleidaten beschränkende Auswirkungen auf die wirtschaftliche Entfaltung der Beschwerdeführer. Die wirtschaftliche Betätigung als Ausprägung der durch Art. 2 Abs. 1 GG geschützten allgemeinen Handlungsfreiheit genießt grundrechtlichen Schutz."[1043]

Für eine generelle Einbeziehung der Berufsgeheimnisse in den Schutzbereich des Art. 12 I GG könnten folgende Überlegungen sprechen: Die hier in Rede stehenden

1040 Siehe BVerfG, Beschluss vom 12.04.2005, Az.: 2 BvR 1027/02, Rn. 94; gleiches soll auch für den Steuerberater gelten, vgl. ebenda Rn. 96.
1041 BVerfG, Urteil vom 30.03.2004, Az.: 2 BvR 1520/01 und 1521/01, Rn. 104.
1042 BVerfG, Beschluss vom 12.04.2005, Az.: 2 BvR 1027/02, Rn. 94.
1043 BVerfG, Beschluss vom 12.04.2005, Az.: 2 BvR 1027/02, Rn. 95.

Sonderberufsgeheimnisse, also die Berufsgeheimnisse, die vor allem dem Schutz des zugrundeliegenden Vertrauensverhältnisses dienen,[1044] haben hinsichtlich des zu Grunde liegenden Berufsbilds regelmäßig eine Typisierung durch den Gesetzgeber bezüglich Ausbildung, Abrechnung, Standesrecht und ähnlichem erfahren (Wirtschaftsprüfer, vereidigte Buchprüfer, Psychologen, Schwangerenberater, Sozialarbeiter etc.).[1045] Dazu gehört in der Regel gerade auch das besondere Vertraulichkeitsgebot, das etwa durch § 203 I StGB strafrechtlich geschützt wird und nach § 53 I S. 1 StPO zur Zeugnisverweigerung berechtigt. Die Einhaltung des Vertraulichkeitsgebots stellt also konstituierenden Teil dieser jeweiligen Berufsausübung dar und ist untrennbar mit dieser verbunden – de facto und nach dem beruflichen Selbstverständnis. Daher sind auch Berufsgeheimnisse vom Schutzbereich der Berufsfreiheit (Art. 12 I GG) erfasst.

2. Grundrechtseingriff durch ein absolutes Verschlüsselungsverbot

Ein absolutes Verschlüsselungsverbotsgesetz würde einen Eingriff in die Berufsfreiheit darstellen, da bestimmte berufliche Betätigungen verboten würden bzw. die Berufsausübung von Berufsgeheimnisträgern beeinflusst würde.

3. Verfassungsrechtliche Rechtfertigung eines absoluten Verschlüsselungsverbots

a. Gesetzesvorbehalt

Der Eingriff in die Berufsfreiheit könnte verfassungsrechtlich gerechtfertigt werden. Ein Eingriff in Art. 12 I GG kann nur durch oder auf Grund eines Gesetzes erfolgen (Art. 12 I S. 2 GG, der zwar ausdrücklich nur die Berufsausübung nennt, sich aber auch auf die Berufswahl bezieht[1046]). Hier wird die Regelung eines absoluten Verschlüsselungsverbots durch ein formelles Gesetz unterstellt.

b. Verhältnismäßigkeitsgrundsatz

Ein solches Gesetz müsste vor allem dem Verhältnismäßigkeitsgrundsatz genügen. Ein absolutes Verschlüsselungsverbot dient *legitimen Zwecken*: Prävention und Verfolgung von Straftaten sowie Sicherung des Rechtsfriedens durch die Verfolgung und Verhütung von Straftaten. Bereits erörtert wurden die Zweifel an der *Geeignet-*

1044 Vgl. zur Terminologie *Kloepfer,* Informationsrecht, § 9, Rn. 67, 80.
1045 Aufzählung nach *Kloepfer,* Informationsrecht, § 9, Rn. 83.
1046 BVerfGE 7, 377, 378 (5. Leitsatz) sowie 401 ff.; ausführlich dazu *Gubelt*, in: *v. Münch/Kunig,* GG, Art. 12, Rn. 41, 44.

heit eines Verschlüsselungsverbots zur Erreichung dieser Zwecke. Von der *Erforderlichkeit* ist dagegen auszugehen.

Die *Verhältnismäßigkeit im engeren Sinne* orientiert sich im Rahmen der Berufsfreiheit nach wie vor[1047] an der vom BVerfG entwickelten Drei-Stufen-Theorie,[1048] wobei sich eine stärkere Rückbesinnung auf den zugrunde liegenden Verhältnismäßigkeitsgrundsatz und damit einhergehend eine zunehmende Flexibilisierung abzuzeichnen scheint.[1049] Danach sind Berufsausübungsregelungen zunächst zulässig, „soweit vernünftige Erwägungen des Gemeinwohls es zweckmäßig erscheinen lassen."[1050] Allerdings ist auch immer wieder betont worden, dass es Berufsausübungsregelungen höchst unterschiedlicher Eingriffsqualität geben kann.[1051] So wird vom BVerfG in Fällen, in denen die Berufsausübungsregelung so schwerwiegend ist, dass sie nicht nur in Einzelfällen zur Berufsaufgabe zwingt, verlangt, dass die Maßstäbe einer Berufswahlregelung eingehalten werden:[1052]

> „Bei der weiteren Prüfung ist daher davon auszugehen, daß das Verbot zwar als bloße Regelung der Berufsausübung zu beurteilen ist, daß es aber wegen seiner Auswirkungen einem Eingriff in die Freiheit der Berufswahl nahekommt und daß es demgemäß nicht mit jeder vernünftigen Erwägung des Gemeinwohls, sondern nur mit solchen Allgemeininteressen gerechtfertigt werden kann, die so schwer wiegen, daß sie den Vorrang vor der Berufsbehinderung der Präparatoren verdienen."[1053]

Letztlich ergibt sich damit auch im Bereich der Berufsfreiheit keine signifikante Abweichung zu der üblichen Abwägung der betroffenen Rechtsgüter und Interessen im Rahmen der Verhältnismäßigkeit im engeren Sinne. Die Grundrechtsbeeinträchtigungen müssen in angemessenem Verhältnis zu den verfolgten Gemeinwohlinteressen stehen.

- Die Auswirkungen eines absoluten Verschlüsselungsverbotsgesetzes auf Entwickler, Hersteller und Verkäufer von Verschlüsselungsprodukten wären zumindest teilweise äußerst gravierend. Im Bereich der IT-Sicherheit wäre eine völlige Neuausrichtung in Forschung und Entwicklung erforderlich, da die Erreichung bestimmter IT-Sicherheitsziele nach derzeitigem Stand der Technik allein über Verschlüsselungsverfahren realisiert wird. Daraus resultierende grundlegende Umwälzungen im Markt „IT-Sicherheit" können ohne Weiteres prognostiziert werden. Damit liegt auf der Hand, dass es nicht nur vereinzelt zu

1047 *Wieland*, in: *Dreier,* GG, Art. 12, Rn. 116.

1048 Diese wurde durch das Apothekenurteil (BVerfGE 7, 377) begründet; ausführlich dazu sowie zu Kritikpunkten und Modifikationen in der Rechtsprechung *Manssen*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 12, Rn. 124, 138 ff.; *Gubelt*, in: *v. Münch/Kunig,* GG, Art. 12, Rn. 44 ff.; *Wieland*, in: *Dreier,* GG, Art. 12, Rn. 107 ff.; *Mann*, in: *Sachs*, GG, Art. 12, Rn. 125 ff.

1049 So jedenfalls *Wieland*, in: *Dreier,* GG, Art. 12, Rn. 116.

1050 BVerfGE 7, 377, 405.

1051 *Manssen*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 12, Rn. 142.

1052 So auch im Fall der bereits oben beispielhaft erwähnten Besitz-, Verarbeitungs- und Vertriebsverbote hinsichtlich bestimmter artengeschützter Tiere: BVerfGE 61, 291, 311 – Tierpräparatoren; *Manssen*, in: *v. Mangoldt /Klein/Starck,* GG, Art. 12, Rn. 142 m.w.N.

1053 BVerfGE 61, 291, 311.

Auswirkungen kommen wird, die einem Eingriff in die Berufswahl nahekommen.

- Die Berufsgeheimnisträger wären demgegenüber zwar eindeutig nur in ihrer Berufsausübungsfreiheit betroffen. Es sind aber die Grundbedingungen ihrer Berufsausübung betroffen. Ein absolutes Verschlüsselungsverbot würde Berufsgeheimnisträgern zum einen die effektivste Möglichkeit zur Gewährleistung der Vertraulichkeit der Daten ihrer Kunden, Mandanten oder Patienten nehmen. Zum anderen wäre die Nutzung bestimmter Informations- und Kommunikationskanäle erschwert oder unmöglich: Die Nutzung von E-Mail wäre ohne entsprechende Vertraulichkeitssicherung durch Verschlüsselung schwerlich mit dem Vertraulichkeitsgebot vereinbar.[1054] Informations- und Hilfsangebote könnten zwar via Internet bereitgestellt werden, deren Nutzung durch Hilfesuchende könnte aber erschwert werden, wenn unbeobachtetes Sich-Informieren nicht möglich ist – gerade bei medizinischen oder psychologischen Fragen.[1055] Diesen Einschüchterungseffekten kommt zusätzliches eigenständiges Gewicht zu.

Diese bedeutenden Grundrechtsbeeinträchtigungen sollen zwar der Wahrnehmung gewichtiger Allgemeinwohlbelange dienen. Inwiefern diese Allgemeinwohlbelange aber tatsächlich gewahrt werden ist angesichts vielfältiger Umgehungsmöglichkeiten und der ungewissen Effizienz von Kommunikationsüberwachungsmaßnahmen zweifelhaft.[1056] Schließlich sind auch mögliche alternative Ermittlungsansätze sowie sicherheitsbehördliche Kenntnisnahmemöglichkeiten trotz des Einsatzes von Verschlüsselung bei der Abwägung zu berücksichtigen.[1057] Darin liegt kein angemessenes Verhältnis der Grundrechtsbeeinträchtigungen zu den verfolgten Gemeinwohlinteressen. Der Eingriff in die Berufsfreiheit (Art. 12 I GG) ist nicht verfassungsrechtlich zu rechtfertigen.

4. Ergebnis

Ein absolutes Verschlüsselungsverbotsgesetz würde daher gegen die Berufsfreiheit (Art. 12 I GG) verstoßen.

1054 Mit dieser Aussage soll nicht behauptet werden, dass sich aus den (standesrechtlichen) Verschwiegenheitspflichten bestimmter Berufsgruppen eine Pflicht zur Verschlüsselung ergibt: Wäre Verschlüsselung verboten, könnte das Berufsrecht deren Einsatz auch nicht fordern. Hier wird vielmehr eine objektive Betrachtungsweise jenseits subjektiver Pflichten eingenommen. Dann kann die Nutzung eines unsicheren Kommunikationsmediums nicht als vertraulichkeitswahrend angesehen werden.

1055 Vgl. nochmals Arbeitskreis Vorratsdatenspeicherung, Pressemitteilung vom 03.06.2008, verfügbar unter: http://www.daten-speicherung.de/data/forsa_2008-06-03.pdf (04.06.2008). In dieser Umfrage gab mehr als die Hälfte der Befragten an, im Hinblick auf die Vorratsdatenspeicherung nicht per Telefon oder E-Mail Kontakt zu bestimmten Einrichtungen wie Drogen- oder Eheberatungsstellen aufzunehmen.

1056 Siehe oben unter A.I.3.c.dd)(6) und (7).

1057 Siehe oben unter A.I.3.c.dd)(8) und (9).

Daneben könnte ein absolutes Verschlüsselungsverbotsgesetz auch einen Verstoß gegen die in Art. 2 I GG als Ausprägung der allgemeinen Handlungsfreiheit geschützte wirtschaftliche Betätigungsfreiheit[1058] darstellen. Da die Schutzbereiche der Eigentums- und der Berufsfreiheit eröffnet sind, ist für die Anwendung der allgemeinen Handlungsfreiheit als grundsätzlich subsidiäres Auffanggrundrecht kein Raum.[1059] Soweit das BVerfG den eventuellen Verlust von Mandanten auf Grund enttäuschter Vertraulichkeitserwartungen allein durch die wirtschaftliche Betätigungsfreiheit (Art. 2 I GG) geschützt gesehen hat,[1060] kann dieser Einordnung nicht gefolgt werden: Da die Berufsgeheimnisse nach hier vertretener Auffassung vom Schutzbereich der Berufsfreiheit (Art. 12 I GG) umfasst sind (und nicht wie teilweise vom BVerfG vertreten als Bestandteil des Rechts auf ein rechtstaatlich faires Verfahren[1061]), müssen auch die Folgen enttäuschter Vertraulichkeitserwartungen für die Berufsausübung (Verlust von Mandanten, eventuell Verlust des „guten Rufs", Verdiensteinbußen) an Art. 12 I GG gemessen werden.

Auch wenn man das Grundrecht auf wirtschaftliche Betätigungsfreiheit hier neben den Spezialgrundrechten aus Art. 12 I GG und Art. 14 I S. 1 GG für anwendbar halten würde, dürfte sich in der Sache nichts anderes ergeben: Es herrscht Einigkeit darüber, dass Berufs- und Eigentumsfreiheit im Verhältnis der Spezialität zur wirtschaftlichen Betätigungsfreiheit stehen.[1062] Dann müsste man aber – wie dies etwa für das Verhältnis von Art. 10 I GG und Art. 13 I GG zum Recht auf informationelle Selbstbestimmung (Art. 2 I GG i.V.m. Art. 1 I GG) entschieden wurde[1063] – beson-

1058 *Kunig*, in: *v. Münch/Kunig,* GG, Art. 2, Rn. 16; *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 145 ff.; *Dreier*, in: *Dreier,* GG, Art. 2 I, Rn. 38.

1059 So auch *Kunig*, in: *v. Münch/Kunig,* GG, Art. 2, Rn. 16, 88 ff.; *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 100; *Wieland*, in: *Dreier,* GG, Art. 12, Rn. 175

1060 S.o. unter II.1.b. sowie BVerfG, Beschluss vom 12.04.2005, Az.: 2 BvR 1027/02, Rn. 95: „Es besteht zudem die Gefahr, dass Mandanten, welchen der Zugriff der Strafverfolgungsbehörden auf auch sie betreffende und regelmäßig vertrauliche Daten bekannt wird, das Mandatsverhältnis zu ihrem Rechtsanwalt oder Steuerberater kündigen. Damit hat der Zugriff auf die Kanzleidaten beschränkende Auswirkungen auf die wirtschaftliche Entfaltung der Beschwerdeführer. Die wirtschaftliche Betätigung als Ausprägung der durch Art. 2 Abs. 1 GG geschützten allgemeinen Handlungsfreiheit genießt grundrechtlichen Schutz."

1061 S.o. unter II.1.b. sowie BVerfG, Beschluss vom 12.04.2005, Az.: 2 BvR 1027/02, Rn. 88.

1062 *Kunig*, in: *v. Münch/Kunig,* GG, Art. 2, Rn. 16; *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 146, 147; *Dreier*, in: *Dreier,* GG, Art. 2 I, Rn. 38; *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 100.

1063 Vgl. BVerfG, Urteil vom 04.04.2006, Az.: 1 BvR 518/02, Rn. 95, in dem das BVerfG Kriterien, die aus den Spezialgrundrechten entwickelt wurden, auf das allgemeine Grundrecht übertragen hat: „Das Bundesverfassungsgericht hat diese Kriterien für die Bemessung der Eingriffsintensität informationsbezogener Grundrechtseingriffe bislang vor allem in Entscheidungen zum Fernmeldegeheimnis aus Art. 10 Abs. 1 GG und zum Grundrecht der Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG entwickelt. Da diese Grundrechte spezielle Ausprägungen des Grundrechts auf informationelle Selbstbestimmung darstellen, sind die-

dere Beurteilungsmaßstäbe der Spezialgrundrechte auf das allgemeine Grundrecht der wirtschaftlichen Betätigungsfreiheit übertragen, will man die spezialgrundrechtliche Konturierung nicht leer laufen lassen.[1064] Schließlich entspricht dem weiten Anwendungsbereich der wirtschaftlichen Betätigungsfreiheit eine großzügige Beschränkungsmöglichkeit.[1065] Die Entscheidung, ob ein bestimmter Eingriff einen Verstoß gegen die wirtschaftliche Betätigungsfreiheit darstellt, fällt mithin auf Verhältnismäßigkeitsebene. Hier stehen sich dieselben Positionen und Argumente gegenüber wie auch im Rahmen der Berufsfreiheit und der Eigentumsfreiheit. Im Ergebnis liegt kein Verstoß gegen die wirtschaftliche Betätigungsfreiheit (Art. 2 I GG) vor, da bereits deren Geltungsbereich nicht eröffnet ist.

IV. Weitergehender Schutz besonderer Berufsgeheimnisse?

Zu prüfen ist, inwieweit sich aus weiteren Grundrechten mit Bezug zur beruflichen Betätigung weitergehender Schutz für besondere Vertraulichkeitsverhältnisse ergeben kann. Neben dem Redaktionsgeheimnis als besonderem, aus der Pressefreiheit (Art. 5 I S. 2 GG) herrührendem Geheimnisschutz (siehe sogleich unter 1.) und dem Beichtgeheimnis als besonderem Geheimnisschutz aus der Religionsfreiheit (Art. 4 I GG) (2.), könnte sich vor allem aus dem Abgeordnetenstatus nach Art. 38 I S. 2 GG (3.), dem freien Mandat, ein weitergehender Schutz von Berufsgeheimnissen ergeben. Schließlich kommt ein besonderer Geheimnisschutz auch hinsichtlich der Forschungsfreiheit (Art. 5 III S. 1 GG) in Betracht (4.).

1. Pressefreiheit (Art. 5 I S. 2 GG)

Die Pressefreiheit schützt als wesentlichen Bestandteil das Redaktionsgeheimnis sowie die Vertraulichkeit von Pressekontakten, sei es mit Informanten, sei es mit Personen, über die berichtet wird:[1066]

> „Die Gewährleistungsbereiche der Presse- und der Rundfunkfreiheit schließen diejenigen Voraussetzungen und Hilfstätigkeiten mit ein, ohne welche die Medien ihre Funktion nicht in angemessener Weise erfüllen können. Geschützt sind namentlich die Geheimhaltung der Informationsquellen und das Vertrauensverhältnis zwischen Presse beziehungsweise Rundfunk und den Informanten. Staatlichen Stellen ist es darüber hinaus grundsätzlich verwehrt, sich Einblick in die Vorgänge zu verschaffen, die zur Entstehung von Nachrichten oder Beiträgen führen, die in der Presse gedruckt oder im Rundfunk gesendet werden. Deshalb besteht auch ein schutzwürdiges Interesse der Medien an der Geheimhaltung solcher Unterlagen, die das Er-

se Maßstäbe auch auf das allgemeinere Grundrecht anwendbar, soweit sie nicht durch die für die speziellen Gewährleistungen geltenden Besonderheiten geprägt sind."

1064 Zwar nicht explizit diese Schlussfolgerung formulierend, aber doch mit parallelem Problembewusstsein *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 100.

1065 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 147.

1066 Ausführlich dazu *Degenhart*, in: *Dolzer/Vogel,* BK-GG, Art. 5 I, II, Rn. 399 ff.

gebnis eigener Beobachtungen und Ermittlungen sind. Geschützt ist auch der Kontakt zu Personen, die selbst Gegenstand der Berichterstattung sind."[1067]

Das Verhältnis von Presse- und Berufsfreiheit ist nicht abschließend geklärt. Zum Teil werden die Grundrechte von einer Literaturmeinung als idealkonkurrierend nebeneinanderstehend angesehen.[1068]Andere Stimmen in der Literatur betonen, dass die Pressefreiheit eine spezielle Berufsfreiheit sei und die Pressefreiheit insoweit auch hinsichtlich des berufsfreiheitsrechtlichen Gehalts lex specialis zu Art. 12 I GG sei.[1069] Schließlich gibt es Stimmen, die ergebnisorientiert danach fragen, ob sich im Hinblick auf die Schrankenregelung des Art. 5 II GG ein im Verhältnis zur Berufsfreiheit weitergehender Schutz durch die Pressefreiheit ergibt. Für diesen Fall soll die Pressefreiheit vorrangig sein, andernfalls – soweit „Regelungen mit berufsregelnder Tendenz die Presse spezifisch betreffen"[1070] – soll Idealkonkurrenz[1071] vorliegen.[1072]

Im Hinblick auf das hier diskutierte absolute Verschlüsselungsverbotsgesetz ergibt sich in der Sache keine im Vergleich zur Berufsfreiheit abweichende Beurteilung. Ein derartiges Verschlüsselungsverbot würde ein allgemeines Gesetz im Sinne von Art. 5 II GG darstellen,[1073] da es gleichermaßen für alle Presseorgane gelten würde und dem Schutz eines bedeutenden Gemeinschaftswerts dienen soll. Auf der Ebene der Verhältnismäßigkeit wäre aber im Kern dieselbe Abwägungsentscheidung zu treffen wie im Rahmen der Berufsfreiheit, des Fernmeldegeheimnisses oder des allgemeinen Persönlichkeitsrechts: Die Rechtsgüter, die ein absolutes Verschlüsselungsverbot schützen soll, sind an sich so hochrangig, dass sie den Eingriff in die Pressefreiheit rechtfertigen könnten. Dass sie dies nach hier vertretener Auffassung

1067 BVerfG, Urteil vom 12.03.2003, Az.: 1 BvR 330/96 und 348/99, Rn. 103, 104.

1068 *Schulze-Fielitz*, in: *Dreier,* GG, Art. 5 I, II, Rn. 318; *Scholz*, in: *Maunz/Dürig,* GG, Art. 12, Rn. 170; *Wendt*, in: *v. Münch/Kunig,* GG, Art. 5, Rn. 115; *Gubelt*, in: *v. Münch/Kunig,* GG, Art. 12, Rn. 95, der aber bei vollständiger oder überwiegender Zielrichtung einer Maßnahme auf nur eines der beiden Grundrechte, allein dieses Grundrecht prüfen will unter „Mitberücksichtigung" des anderen.

1069 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 5, Rn. 285; ebenso wohl auch *Kloepfer,* Informationsrecht, § 3, Rn. 57.

1070 *Degenhart*, in: *Dolzer/Vogel,* BK-GG, Art. 5 I, II, Rn. 942.

1071 Eine Schutzbereichsverstärkung von Art. 12 I GG wurde dagegen soweit ersichtlich nicht diskutiert. Es besteht im Rahmen der Berufsfreiheit auch keine wesentlich veränderte Gefährdungslage (wie dies beim allgemeinen Persönlichkeitsrecht mit den Möglichkeiten der Datenverknüpfung und Profilbildung der Fall ist), die eine solche Schutzbereichsverstärkung angezeigt erscheinen lassen würde. Es ergeben sich keine besonderen Gefahren für die Berufsfreiheit im Allgemeinen durch eine Betroffenheit der Presse im Speziellen. Wie im Verhältnis von Art. 2 I GG i.V.m. Art. 1 I GG zu Art. 10 I GG und Art. 13 I GG haben diese Gewährleistungen schon immer in der geschilderten Weise miteinander konkurriert, ohne dass sich irgendwelche Änderungen ergeben hätten, die eine andere Perspektive erforderlich machen würden. Gleiches gilt für die im Folgenden diskutierte Religionsfreiheit, die Wissenschaftsfreiheit und die Freiheit des Mandats.

1072 *Degenhart*, in: *Dolzer/Vogel,* BK-GG, Art. 5 I, II, Rn. 942.

1073 Vgl. zur alten Streitfrage, wann ein allgemeines Gesetz in diesem Sinne vorliegt, den Überblick bei *Schulze-Fielitz*, in: *Dreier,* GG, Art. 5 I, II, Rn. 136 ff.

im Ergebnis doch nicht können, liegt weniger an der Wertigkeit der Rechtsgüter an sich als am Verhältnis von realisierbarem Schutz des Rechtsguts zu den daraus resultierenden Grundrechtseingriffen, ist also eindeutig eine Frage der Verhältnismäßigkeit. Es geht um dieselben Rechtspositionen und Abwägungsbelange. Daher kann offen bleiben, ob die Pressefreiheit für das pressespezifische Berufsgeheimnis lex specialis zur Berufsfreiheit ist oder beide Grundrechte insoweit nebeneinander stehen: Im Ergebnis würde ein absolutes Verschlüsselungsverbot jedenfalls ebenso gegen die Pressefreiheit (Art. 5 I S. 2 GG) verstoßen.

2. Religionsfreiheit (Art. 4 I GG)

Der Schutz der Religionsfreiheit (Art. 4 I GG) umfasst ebenfalls den Schutz eines besonderen Berufsgeheimnisses, nämlich des Beichtgeheimnisses.[1074] Im weiteren Sinne ist aber nicht nur das kirchenrechtliche Beichtgeheimnis geschützt, sondern auch sonstige religiöse Kommunikation, insbesondere mit Geistlichen.[1075] Dieser besondere Vertraulichkeitsschutz soll insgesamt in den Schutzbereich der Religionsfreiheit fallen, welche Art. 12 I GG insoweit als lex specialis verdrängen soll.[1076] Zum Teil wird - wie auch für das Verhältnis von Presse- und Berufsfreiheit – vertreten, dass Art. 4 I GG neben anderen Grundrechten anwendbar sei. Hinsichtlich des effektiven Grundrechtsschutzes sei dann häufig die Religionsfreiheit wegen ihrer vorbehaltlosen Gewährleistung maßgeblich.[1077] Die Diskussion dreht sich dabei zumeist aber nur um wirtschaftliche Betätigung, die gleichzeitig Religionsausübung darstellt.[1078] Soweit explizit Einschränkungen religiöser Berufsausübung (etwa als Geistlicher) thematisiert werden, wird die Religionsfreiheit als vorrangig vor der Berufsfreiheit erachtet.[1079] Der Schutzbereich ist jedenfalls eröffnet.

Die Religionsfreiheit wird dem Wortlaut nach vorbehaltlos gewährleistet.[1080] Nach der Rechtsprechung des BVerfG und Stimmen in der Literatur ist aber auch die Religionsfreiheit nicht schrankenlos, sondern findet ihre Grenze an den verfassungsimmanenten Schranken.[1081] Nach einer anderen Literaturmeinung wird die Religionsfreiheit durch die „bürgerlichen und staatsbürgerlichen Pflichten“ des über Art. 140 GG inkorporierten Art. 136 I Weimarer Reichsverfassung einge-

1074 *Kloepfer,* Informationsrecht, § 3, Rn. 57.
1075 Den Schutz des Gesprächs mit Geistlichen durch die Religionsfreiheit betonend auch BVerfG, Beschluss vom 11.05.2007, Az.: 2 BvR 543/06, Rn. 36.
1076 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 4, Rn. 158.
1077 So *Morlok*, in: *Dreier,* GG, Art. 4, Rn. 188.
1078 Siehe etwa *Mager*, in: *v. Münch/Kunig,* GG, Art. 4, Rn. 90; *Morlok*, in: *Dreier,* GG, Art. 4, Rn. 189.
1079 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 4, Rn. 158.
1080 *Mager*, in: *v. Münch/Kunig,* GG, Art. 4, Rn. 46; *Morlok*, in: *Dreier,* GG, Art. 4, Rn. 111; *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 4, Rn. 84.
1081 *Mager*, in: *v. Münch/Kunig,* GG, Art. 4, Rn. 47; *Morlok*, in: *Dreier,* GG, Art. 4, Rn. 112.

schränkt.[1082] Im Ergebnis kommt es hier aber nicht darauf an, welcher der beiden Auffassungen zu folgen ist. Bei einem absoluten Verschlüsselungsverbotsgesetz geht es um die Aufrechterhaltung sicherheitsbehördlicher Kenntnisnahmeoptionen zur Prävention und Repression von Straftaten sowie die Schaffung von Rechtsfrieden durch die Verfolgung und Ahndung von Straftaten. Straf- und strafprozessrechtliche wie gefahrenabwehrrechtliche Normen könnten nach beiden Auffassungen die Religionsfreiheit einschränken: Solche Normen sind einerseits allgemeine „bürgerliche und staatsbürgerliche Pflichten“ (Art. 140 GG i.V.m. Art. 136 i WRV)[1083] und andererseits Ausdruck der Erfüllung staatlicher Schutzpflichten zum Schutz von Leben und körperlicher Unversehrtheit (Art. 2 II S. 1 GG)[1084] – mithin kollidierendes Verfassungsrecht:

> „Daher ist der Staat gemäß Art. 1 Abs. 1 S. 2 verpflichtet, das menschliche Leben auch gegen Angriffe Dritter zu schützen […] Hierzu gehört der Einsatz des repressiv wirkenden Strafrechts und, soweit Angriffe gegen das Leben abgewehrt werden können, das präventiv wirkende Polizeirecht sowie die Unterhaltung einer aktionsfähigen Polizei.“[1085]

Daher ist im Ergebnis jeweils die altbekannte Abwägung zwischen den widerstreitenden Belangen zu leisten. Im Ergebnis verstieße ein absolutes Verschlüsselungsverbot folglich auch gegen die Religionsfreiheit (Art. 4 I GG).

3. Freiheit des Mandats (Art. 38 I S. 2 GG)

Aus dem Status als Abgeordneter des Bundestags nach Art. 38 I S. 2 GG ergibt sich ebenfalls ein besonderes Berufsgeheimnis. Dies verdeutlicht etwa das strafprozessuale Zeugnisverweigerungsrecht für Abgeordnete hinsichtlich aller Tatsachen, die ihnen in dieser Eigenschaft anvertraut wurden, nach § 53 I S. 1 Nr. 4 StPO.[1086] Die Freiheit des Mandats kann durch andere Rechtsgüter von Verfassungsrang beschränkt werden.[1087] Prävention und Verfolgung von Straftaten können dabei grundsätzlich Eingriffe in das freie Mandat rechtfertigen.[1088] Die zwischen den Rechtsgü-

1082 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 4, Rn. 87 f.

1083 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 4, Rn. 96, 103.

1084 Zur staatlichen Verpflichtung, Leben und körperliche Unversehrtheit (Art. 2 II S. 1 GG) durch strafrechtliche Sanktionen zu schützen vgl. *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 2, Rn. 214 und 236.

1085 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 1, Rn. 92.

1086 So auch Bundestagsfraktion von Bündnis 90/Die Grünen, Antragsschriftsatz vom 08.02.2008 im Organstreitverfahren, Az.: 2 BvE 1/08 gegen die Vorratsdatenspeicherung, verfügbar unter: http://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV14-1795.pdf?von=1&bis=0 (03.09.2008), S. 9.

1087 *Morlok*, in: *Dreier,* GG, Art. 38, Rn. 151; Bundestagsfraktion von Bündnis 90/Die Grünen, Antragsschriftsatz vom 08.02.2008 im Organstreitverfahren, Az.: 2 BvE 1/08 gegen die Vorratsdatenspeicherung, verfügbar unter: http://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV14-1795.pdf?von=1&bis=0 (03.09.2008), S. 27.

1088 So ebenfalls Bundestagsfraktion von Bündnis 90/Die Grünen, Antragsschriftsatz vom 08.02.2008 im Organstreitverfahren, Az.: 2 BvE 1/08 gegen die Vorratsdatenspeicherung, verfügbar

tern zu treffende Abwägungsentscheidung verläuft im Wesentlichen parallel zur jeweiligen Abwägung im Rahmen der bereits dargestellten besonderen Berufsgeheimnisse. Wenn man nicht bereits die Eröffnung des Schutzbereichs verneinen möchte, weil man den Schutz von Berufsgeheimnissen in Art. 12 I GG verortet, würde ein absolutes Verschlüsselungsverbot daher auch einen Verstoß gegen die Freiheit des Mandats (Art. 38 I S. 2 GG) darstellen – sei es als lex specialis zur Berufsfreiheit, sei es neben dieser.

4. Wissenschaftsfreiheit (Art. 5 III S. 1 GG)

Zuletzt könnte sich auch aus der Wissenschaftsfreiheit (Art. 5 II S. 1 GG) ein besonderes Berufsgeheimnis ergeben. Zunächst würde sich aus einem absoluten Verschlüsselungsverbotsgesetz allein deshalb ein Eingriff in die Wissenschaftsfreiheit (Art. 5 III S. 1 GG) ergeben, weil Forschung an Verschlüsselungsverfahren damit untersagt würde:

> „Jedes Verbot von Forschung oder Lehre, jede staatliche Einflußnahme auf Fragestellung, Methode, Materialsammlung, Bewertung und Verbreitung der Ergebnisse bei der Forschung, jede Steuerung oder Kontrolle von Inhalt und Ablauf der Lehre sind als Beeinträchtigung der Wissenschaftsfreiheit anzusehen.“[1089]

Die Wissenschaftsfreiheit gewährleistet also einen originären Schutz von Verschlüsselungsverfahren. Zu prüfen ist, ob die Wissenschaftsfreiheit darüber hinaus auch die Geheimhaltung von Forschung (und damit einen derivativen Schutz von Verschlüsselung) umfasst. Dies wurde zum Teil in der Literatur verneint, da Forschung wesentlich durch ihre Veröffentlichung, fachliche Diskussion und Kontrolle bestimmt sei:

> „Im übrigen ist die Forschungsfreiheit auf die Möglichkeit der Publikation der Forschungsergebnisse hin angelegt, während das Berufs- und Geschäftsgeheimnis gerade geheim gehalten werden muß, um seinen Vermögenswert im Wettbewerb zu erhalten.“[1090]

Andererseits ist auch die Wissenschaft durchaus von einem Wettbewerbsverhältnis der Akteure gekennzeichnet – um Forschungsmittel wie wissenschaftliche Reputation. Es handelt sich um einen Wettbewerb der Ideen, an denen – jedenfalls bis zu einer Veröffentlichung – durchaus ein berechtigtes Geheimhaltungsinteresse besteht. Schließlich schließt eine (zeitlich begrenzte) Geheimhaltung nicht per se aus, dass der Schutzbereich der Wissenschaftsfreiheit betroffen ist: So soll – relevant vor al-

unter: http://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/M MV14-1795.pdf?von=1&bis=0 (03.09.2008), S. 27 mit dem Hinweis darauf, dass auch die Immunität der Abgeordneten gerade keine absolute sei (vgl. den Wortlaut von Art. 46 II GG) und insbesondere zur Strafverfolgung häufig aufgehoben wird (vgl. die Zahlen bei *Schulze-Fielitz*, in: *Dreier,* GG, Art. 46, Rn. 36).

1089 *Pernice*, in: *Dreier,* GG, Art. 5 III, Rn. 38 unter beispielhafter Nennung etwa des Stammzell-Gesetzes.

1090 *Berg,* GewArch 1996, 177, 178.

lem in der Auftragsforschung – nur eine zeitlich unbegrenzte Publikationssperre gegen die Annahme von Wissenschaft im Sinne des Art. 5 III S. 1 GG sprechen.[1091] Anerkannt ist weiter auch die negative Wissenschaftsfreiheit, also die dauerhafte Nicht-Veröffentlichung bestimmter Forschung (etwa aus ethischen Gründen).[1092] Grenze wäre nur die beabsichtigte, systematische Nicht-Veröffentlichung von Forschungsergebnissen, da der Wissenschaftsbegriff auch durch den kritischen Diskurs innerhalb der *`scientific community´* geprägt ist.[1093] Der Wissenschaftsbegriff steht daher der Annahme eines Berufsgeheimnisses von Wissenschaftlern nicht entgegen.

Ein wissenschaftlicher Geheimnisschutz ist vielmehr nicht nur im Hinblick auf die Eigeninteressen des Wissenschaftlers, seine Ideen bis zu einer Veröffentlichung zunächst geheim zu halten, sondern zum Teil auch im Hinblick auf den Schutz von Daten Dritter erforderlich. Nach einer Literaturmeinung kann sich aus diesem Vertraulichkeitserfordernis in Ausnahmefällen sogar ein strafprozessuales Zeugnisverweigerungsrecht ergeben.[1094] Ein spezielles Vertraulichkeitsverhältnis zu Dritten wie bei den bereits erörterten besonderen Berufsgeheimnissen mag zwar nicht unbedingt prägend für die Wissenschaftsfreiheit sein, ist dieser danach jedenfalls aber auch nicht fremd. Die berechtigten Geheimnisschutzinteressen sprechen für die Einbeziehung eines Rechts auf Geheimhaltung in den Schutzbereich der Wissenschaftsfreiheit. Es muss sich allerdings noch um Wissenschaft im Sinne des Art. 5 III S. 1 GG handeln, die grundsätzlich auf Veröffentlichung von Forschungsergebnissen und wissenschaftlichen Diskurs gerichtet ist.

Dieses Geheimnisschutzrecht stellt sich aber nicht als besonderes Berufsgeheimnis dar. Eine schützenswerte Vertraulichkeitsbeziehung zu Dritten, wie sie für die Pressefreiheit, die Religionsfreiheit und die Freiheit des Mandats charakteristisch ist, liegt im Rahmen der Wissenschaftsfreiheit nur in seltenen, besonderen Konstellationen vor. Im Übrigen geht es um den Schutz wissenschaftlicher Urheberschaft sowie der wissenschaftlichen „Betriebs- und Geschäftsgeheimnisse". Es besteht also eher eine Parallele zu Art. 14 I GG als zu Art. 12 I GG.[1095] Mag der Wissenschaftler auch eine andere als rein wirtschaftliche Verwertungsweise haben, geht es letztlich doch um den Schutz vermögenswerter Rechte. Schließlich ist für die wirtschaftliche Verwertung von Forschungsergebnissen – etwa im Rahmen von universitären *`Spin-offs´* – anerkannt, dass diese vorrangig unter die Eigentumsfreiheit fällt.[1096] Der wis-

1091 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 5, Rn. 355.

1092 *Pernice*, in: *Dreier,* GG, Art. 5 III, Rn. 31; *Fehling*, in: *Dolzer/Vogel,* BK-GG, Art. 5 III, Rn. 74.

1093 *Pernice*, in: *Dreier,* GG, Art. 5 III, Rn. 31; *Fehling*, in: *Dolzer/Vogel,* BK-GG, Art. 5 III, Rn. 74, wobei für den Bereich der Industrieforschung die Richtigkeitskontrolle durch die Umsetzung der Forschungsergebnisse in die Praxis für ausreichend gehalten wird.

1094 *Fehling*, in: *Dolzer/Vogel,* BK-GG, Art. 5 III, Rn. 75 unter Verweis auf *Greitemann*, Das Forschungsgeheimnis, 2001.

1095 So auch *Fehling*, in: *Dolzer/Vogel,* BK-GG, Art. 5 III, Rn. 271: „Die wissenschaftliche Urheberschaft an Erkenntnissen wird – in Parallele zum allgemeinen Urheberrecht – durch Art. 14 GG, nicht durch Art. 5 Abs. 3 GG geschützt."

1096 So *Berg,* GewArch 1996, 177, 178; *Scholz*, in: *Maunz/Dürig,* GG, Art. 5 III, Rn. 84.

senschaftliche Geheimnisschutz wird trotz der strukturellen Nähe zum durch die Eigentumsfreiheit geschützten Betriebs- und Geschäftsgeheimnis durch die Wissenschaftsfreiheit selbst und nicht durch Art. 14 I GG geschützt. Mag es auch um den Schutz vermögenswerter Rechte gehen und mag die Forschung auch finanzielle Motive haben (wie etwa die Gewinnung von Drittmitteln), steht doch der Wissenschaftscharakter im Vordergrund.[1097] Der Schutzbereich der Wissenschaftsfreiheit (Art. 5 III S. 1 GG) umfasst somit auch ein besonderes wissenschaftliches Geheimnisschutzrecht.

Ein absolutes Verschlüsselungsverbot, welches einen effektiven informationstechnischen Schutz dieser wissenschaftlichen Geheimnisse nach derzeitigem Stand der Technik unmöglich machen würde, würde daher einen Eingriff in die Wissenschaftsfreiheit darstellen. Ein Eingriff in die Wissenschaftsfreiheit ergibt sich des Weiteren aus dem Verbot eines bestimmten Forschungsgegenstandes, der Kryptographie. Ein Eingriff in die Wissenschaftsfreiheit kann zum Schutze anderer verfassungsrechtlich geschützter Rechtsgüter gerechtfertigt sein.[1098] Hier steht der Wissenschaftsfreiheit etwa das Recht auf Leben und körperliche Unversehrtheit (Art. 2 II S. 1 GG) gegenüber. Im Rahmen der zu treffenden Abwägungsentscheidung zwischen den kollidierenden Rechtsgütern wäre ein absolutes Verschlüsselungsverbot unverhältnismäßig und nicht zu rechtfertigen:

> „In dem Verbot unangemessener Grundrechtseingriffe finden auch die Pflichten des Staates zum Schutz anderer Rechtsgüter ihre Grenze. Entsprechende Eingriffsschwellen sind durch eine gesetzliche Regelung zu gewährleisten."[1099]

Daher würde ein absolutes Verschlüsselungsverbotsgesetz im Ergebnis auch gegen die Wissenschaftsfreiheit (Art. 5 III S. 1 GG) verstoßen.

V. Zusammenfassung

Ein absolutes Verschlüsselungsverbotsgesetz verstößt sowohl gegen die Eigentums- wie auch gegen die Berufsfreiheit (Art. 14 I S. 1 GG; Art. 12 I GG). Verschlüsselungsverfahren erfahren in diesem Rahmen sowohl originären Schutz als unmittelbarer Gegenstand des grundrechtlichen Schutzes als auch derivativen Schutz als Mittel zur Gewährleistung der Vertraulichkeit von Betriebs- und Geschäftsgeheimnissen bzw. zum Schutz von Berufsgeheimnissen. Zum Teil sind derartige Geheimnisse aber auch von Spezialnormen wie etwa der Presse- oder der Religionsfreiheit (Art. 5 I S. 2 GG; Art. 4 I GG), der Freiheit des Mandats (Art. 38 I S. 2 GG) oder der Wissenschaftsfreiheit (Art. 5 III S. 1 GG) geschützt. Ein absolutes Verschlüsselungsver-

1097 *Scholz*, in: *Maunz/Dürig,* GG, Art. 5 III, Rn. 84 argumentiert ähnlich für wirtschaftliche Erträge aus Publikations- und Vortragstätigkeit, die so lange unter die Wissenschaftsfreiheit fallen soll als eben Wissenschaft und nicht Profit dafür zweckbestimmend sind.

1098 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 5, Rn. 415; *Pernice*, in: *Dreier,* GG, Art. 5 III, Rn. 40.

1099 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 243.

bot würde mithin auch gegen diese weiteren Grundrechte verstoßen. Eine verfassungsrechtliche Rechtfertigung der Eingriffe scheitert wiederum an der Unverhältnismäßigkeit des Eingriffs. Ein absolutes Verschlüsselungsverbotsgesetz wäre daher auch aus der Perspektive der wirtschaftlichen Betätigung verfassungswidrig.

C. Verschlüsselungsverbot als Gleichheitsverstoß

Schließlich könnte ein absolutes Verschlüsselungsverbotsgesetz einen Verstoß gegen das Willkürverbot (Art. 3 I GG) darstellen. So wurde argumentiert, dass von einem Verschlüsselungsverbot de facto immer nur jene betroffen wären, die erstens technisch wenig versiert sind[1100] und zweitens kein besonderes Interesse an der Sicherung von Vertraulichkeit haben (da sie „nichts zu verbergen haben"). Betroffen von einem absoluten Verschlüsselungsverbotsgesetz wäre mithin immer nur der „unschuldige Dumme", der eventuell gar nicht selbst Anlass der Überwachungsmaßnahme war, sondern von dieser nur „mitbetroffen" wird, während diejenigen, denen die Überwachungsmaßnahme eigentlich gilt und die diese verursacht haben, die Überwachung mit Hilfe von Verschlüsselungsverfahren einfach umgehen (können).[1101]

> „Allerdings ist es in einigen der aufgezählten Gefahrenbereiche naheliegend, daß sich gerade die Zielpersonen oder -organisationen aufgrund ihres hohen Organisationsgrads und der Nutzung moderner Infrastrukturen der Fernmeldeüberwachung zu entziehen vermögen, während Unbeteiligte, die die Verschlüsselungstechniken – wie Journalisten angesichts ihrer Arbeitsbedingungen – nicht nutzen können, von ihr getroffen werden."[1102]

Falls sich die Sachlage in der Praxis überhaupt derart pointiert darstellen sollte, lässt sich jedenfalls daraus allein noch kein Verstoß gegen das Willkürverbot ableiten:

Das zentrale Element eines Verstoßes gegen das Willkürverbot ist nicht die bloße Missachtung des Grundsatzes,

> „Gleiches gleich, Ungleiches seiner Eigenart entsprechend verschieden"[1103]

zu behandeln, sondern vielmehr die *Willkürlichkeit* der Ungleichbehandlung:[1104]

1100 Zu dieser Ausprägung des „digital divide" vgl. Zillien, Zu kurz gesprungen, verfügbar unter: http://www.heise.de/tp/r4/artikel/24/24066/1.html (11.05.2007).

1101 *Koch,* CR 1997, 106, 109. Ebenso wurde auch bei der Frage der Geeignetheit von Internetsperren bezüglich bestimmter unerwünschter Inhalte argumentiert; vgl. *Sieber/Nolde*, Sperrverfügungen im Internet, S. 180 f.

1102 So schon das BVerfG, Urteil vom 14.07.1999, Az.: 1 BvR 2226/94 et al., Rn. 215 zur strategischen Fernmeldeüberwachung.

1103 BVerfGE 3, 58, 135.

1104 *Alexy*, Theorie der Grundrechte, S. 366; *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 3, Rn. 10; *Heun*, in: *Dreier,* GG, Art. 3, Rn. 19.

„Der Gesetzgeber ist an den allgemeinen Gleichheitssatz in dem Sinne gebunden, dass er weder wesentlich Gleiches willkürlich ungleich noch wesentlich Ungleiches willkürlich gleich behandeln darf."[1105]

Im Fall eines absoluten Verschlüsselungsverbotsgesetzes geht es um die faktische Ungleichheit, die aus der mangelnden Kontrolle der Einhaltung des Verbotes resultiert. Die mangelhafte Durchsetzung der materiellen Norm führt zu der beschriebenen faktischen Ungleichheit.[1106] Dies erscheint prima facie willkürlich, da diese Wirkung auf keinerlei sachlichen Grund zurückgeht, mithin schlicht zufällig ist.

Vollzugsmängel führen aber nach der Rechtsprechung des BVerfG – insbesondere zur Steuer- aber auch zur Wehrgerechtigkeit[1107] – nicht automatisch zu einer gleichheitswidrigen rechtlichen und tatsächlichen Ungleichbehandlung. Nur wenn die rechtliche Gestaltung prinzipiell so verfehlt ist, dass sie weitgehend nicht durchgesetzt werden kann, und dies dem Gesetzgeber zuzurechnen ist, liegt nach Auffassung des BVerfG ein Verstoß gegen das Willkürverbot vor:

„Der Gleichheitssatz verlangt für das Steuerrecht, dass die Steuerpflichtigen durch ein Steuergesetz rechtlich und tatsächlich gleich belastet werden. Wird die Gleichheit im Belastungserfolg durch die rechtliche Gestaltung des Erhebungsverfahrens prinzipiell verfehlt, so kann dies die Verfassungswidrigkeit der gesetzlichen Besteuerungsgrundlage nach sich ziehen und die Steuerpflichtigen in ihrem Grundrecht auf Besteuerungsgleichheit verletzen. […] Das ist allerdings nicht schon bei einer Belastungsungleichheit der Fall, die durch Vollzugsmängel bei der Steuererhebung hervorgerufen wird, wie sie immer wieder vorkommen können und sich auch tatsächlich ereignen. Wirkt sich indes eine Erhebungsregelung gegenüber einem Besteuerungstatbestand in der Weise strukturell gegenläufig aus, dass der Besteuerungsanspruch weitgehend nicht durchgesetzt werden kann, und ist dieses Ergebnis dem Gesetzgeber zuzurechnen, so führt die dadurch bewirkte Gleichheitswidrigkeit zur Verfassungswidrigkeit auch der materiellen Norm."[1108]

Da es für die Einhaltung des Verschlüsselungsverbotsgesetzes überhaupt keine Kontrollmechanismen gibt und, wie bereits dargestellt, Verstöße (falls überhaupt) erst anlässlich sicherheitsbehördlicher Abhörmaßnahmen bemerkt werden können, entsteht letztlich eine Situation, die das BVerfG im Bereich steuerverfahrensrechtlicher Vollzugsdefizite wie folgt beschrieben hat:

„Eine solche Weise der Besteuerung wirkt im Ergebnis so, als hätte die Steuer ihren Belastungsgrund letztlich nur in der Bereitschaft, Steuern zu zahlen."[1109]

Auch ein Verschlüsselungsverbot wirkt im Ergebnis nur gegenüber denjenigen, die bereit sind, quasi freiwillig auf die Nutzung von Verschlüsselungsverfahren zu

1105 BVerfGE 4, 144, 155.

1106 Zu den Prinzipien rechtlicher und faktischer Gleichheit vgl. *Alexy*, Theorie der Grundrechte, S. 377 ff. sowie *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 3, Rn. 3 ff.

1107 Angesichts der insbesondere im Rahmen des Gleichheitssatzes zu beachtenden Besonderheiten des jeweiligen Sachbereichs sind derartige sachgebietsübergreifende Vergleiche zwar nur mit äußerster Vorsicht anzustellen. Gleichwohl scheint der Verfasserin eine gewisse Parallelwertung hier möglich, da die Fragestellung der Auswirkungen von Vollzugsdefiziten auf Massenverfahren, denen per se jeder ausgesetzt ist, ähnlich gelagert ist.

1108 BVerfGE 84, 239, Rn. 104, 111.

1109 BVerfGE 84, 239, Rn. 114.

verzichten. Die Entscheidung des BVerfG zur Steuergerechtigkeit ist insofern verallgemeinerungsfähig:[1110]

> „Symbolisches Recht, das seine bloß symbolische Natur nicht auch garantiert, sondern nur den Ehrlichen (oder Dummen, oder Pechvogel) trifft, ist verfassungswidrig."[1111]

Ein absolutes Verschlüsselungsverbotsgesetz wäre also auch wegen Verstoßes gegen das Willkürverbot (Art. 3 I GG) verfassungswidrig.[1112]

1110 So auch *Bryde*, Die Effektivität von Recht als Rechtsproblem, S. 20.

1111 *Bryde*, Die Effektivität von Recht als Rechtsproblem, S. 20.

1112 Anderer Ansicht dürften *Sieber/Nolde*, Sperrverfügungen im Internet, S. 193 ff. sein. Deren Stellungnahme bezieht sich allerdings auf Internetsperren, die sich bei der Frage nach dem Vorliegen von Symbolgesetzgebung doch wesentlich von einem Verschlüsselungsverbot unterscheiden: Internetsperren implementieren keine Strafbarkeit bei Nichtbefolgung des Verhaltensgebots.

Teil 4: Grundrecht auf Verschlüsselung im Kontext eines relativen Verschlüsselungsverbots

Als milderes Mittel im staatlichen Umgang mit Verschlüsselungstechnologien kommt statt eines absoluten Verschlüsselungsverbots auch die alleinige Zulassung der Nutzung von Verschlüsselungsverfahren mit bestimmten Eigenschaften, die staatliche Kenntnisnahmemöglichkeiten sicherstellen, unter Verbot der Nutzung aller übrigen Verfahren in Betracht. Dieses

Szenario 2
Staat S gestattet nur die Nutzung bestimmter Verschlüsselungsverfahren.

wird hier als relatives Verschlüsselungsverbot bezeichnet.[1113] Der Ansatz eines relativen Verschlüsselungsverbots ist wesentlich folgenden Erkenntnissen geschuldet:

- Nicht alle Verschlüsselungsverfahren stehen einer inhaltlichen Kenntnisnahme durch staatliche Sicherheitsbehörden tatsächlich entgegen: Bei Verwendung kurzer Schlüssel[1114] oder bei schwachen Verschlüsselungsverfahren kann durch eine `*Brute-Force´*-Attacke mit vertretbarem Aufwand innerhalb einer vertretbaren Zeitspanne die Verschlüsselung geknackt werden.[1115] Zur Sicherstellung staatlicher Kenntnisnahmeoptionen wäre hinsichtlich solcher Verfahren ein Verschlüsselungsverbot nicht erforderlich. Ein Verschlüsselungsverbot könnte allenfalls als bequemer oder kostengünstiger erscheinen.
- Die Zulassung bestimmter Verschlüsselungsverfahren unter Verbot der übrigen Verfahren könnte sich als Kompromiss zwischen den – auch aus Sicht des Staates – widerstreitenden Interessen darstellen. Denn auch der Staat möchte zwar einerseits seinen Sicherheitsbehörden Kenntnisnahmeoptionen erhalten, hat andererseits aber ebenso Interesse daran, dass etwa Betriebs- und Geschäftsgeheimnisse nicht durch Dritte, insbesondere durch ausländische Geheimdienste,

1113 Relative Verschlüsselungsverbote, die auf einem Zulassungsverfahren in Verbindung mit einem Verbot aller nicht zugelassenen Verschlüsselungsverfahren basieren, wurden teilweise auch als „Lizenzierungsmodelle“ bezeichnet, vergleiche *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 210. Mit der hier verwendeten Terminologie des absoluten und relativen Verschlüsselungsverbots soll die Parallelität beider Regelungsoptionen betont werden.

1114 So wurde laut *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 181 auf die Einflussnahme der US-amerikanischen National Security Agency (NSA) hin die Schlüssellänge für den Data Encryption Standard (DES) verringert – so dass er nun für die NSA knackbar sein dürfte.

1115 Das Knacken von Verschlüsselung durch die Sicherheitsbehörden ist quasi als Annex zu einer Überwachungsbefugnis zulässig, wie *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 193 ff. ausführlich gezeigt hat.

ausgespäht werden können. Entsprechende Schutzpflichten des Staates zum Schutz verfassungsrechtlich geschützter Rechtsgüter stehen sich gegenüber: Hier der Schutz von Leben, körperlicher Unversehrtheit und Freiheit (Art. 2 II S. 1 und 2 GG), dort der Schutz von Privatsphäre (Art. 10 I GG, Art. 13 I GG und Art. 2 I GG i.V.m. Art. 1 I GG) und wirtschaftlicher Betätigung (vor allem Art. 14 I S. 1 GG und Art. 12 I GG).[1116] Ein relatives Verschlüsselungsverbot könnte sich insoweit als Lösung des Dilemmas im Sinne „praktischer Konkordanz" darstellen: Einerseits ist ein gewisser Schutz gegenüber privaten Dritten möglich, andererseits können die Sicherheitsbehörden im Zweifel von den verschlüsselten Inhalten Kenntnis nehmen.

- Neben der Freigabe nur schwacher Verschlüsselungsverfahren bzw. der Verwendung kurzer Schlüssel für den privaten Gebrauch kommen zur Auflösung dieses Konflikts widerstreitender Interessen weitere technische Möglichkeiten in Betracht: So wurde vor allem die Implementierung einer technischen „Hintertür" (`*backdoor´*) in Verschlüsselungsverfahren diskutiert, eine Verpflichtung des Nutzers, Schlüssel zu hinterlegen (häufig als `*key escrow´* oder `*key escrowing´* bezeichnet),[1117] sowie die Implementierung einer Möglichkeit, einen Nachschlüssel zu erzeugen (in den USA unter dem Stichwort `*key recovery´* diskutiert).[1118] Diesen Optionen ist gemein, dass sie von einer *teilnehmerautonomen* Verschlüsselung ausgehen, also der Durchführung des Ver- und Entschlüsselungsvorgangs durch den jeweiligen Nutzer selbst. Die ebenfalls diskutierte Idee, die Anbieter von Verschlüsselungsverfahren zur Aufbewahrung von Schlüsselduplikaten zu verpflichten,[1119] basiert dagegen auf der Prämisse, dass nicht der Nutzer selbst, sondern der Anbieter die Schlüssel generiert (andernfalls hätte der Anbieter keinen Zugriff auf die Schlüssel und könnte keine Schlüsselduplikate speichern).[1120] Schließlich könnten in Fällen der Verschlüsselung durch die Diensteanbieter diesen gesetzliche Mitwirkungspflichten auferlegt

1116 So wurde auch für das Bundesamt für Sicherheit in der Informationstechnik (BSI) von einem Zielkonflikt, der in der Aufgabenzuweisung begründet liegt, gesprochen: „Zwiespältig am BSI ist also weiterhin die ungenügende Trennung zwischen nachrichtendienstlichen und polizeilichen Aufgaben einerseits und denen zur Erhöhung der IT-Sicherheit andererseits. Insbesondere bei Fragen der Kryptographie, aber auch auf anderen Gebieten der IT-Sicherheit gerät das BSI damit in einen Konflikt widersprechender Ziele, wenn der Bedarf nach Sicherheit der Wirtschaft und von Privatpersonen hinter den Interessen von Strafverfolgung und Nachrichtendiensten zurückzustehen hat."; Kleine Anfrage der Fraktion Bündnis 90/Die Grünen zum BSI vom 05.12.1995, BT-Drs. 13/3313, S. 1, 2; mit ähnlichen Argumenten bezeichnet *Bizer,* KritJ 1995, 450, 453 das BSI als „Diener zweier Herren".

1117 Die Idee des `*key escrow´* oder `*key escrowing´* lag auch schon der Clipper-Chip-Initiative in den USA zugrunde, s.o. in Teil 2 unter B.II.

1118 Vgl. zu den verschiedenen Modellen *Andrzejak*, Kryptoregulierung, in: *Hoeren/Queck,* Rechtsfragen der Informationsgesellschaft, S. 132.

1119 Siehe dazu *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 203.

1120 Beispiel ist etwa der GSM-Verschlüsselungsstandard für Handykommunikation.

werden[1121] – wie dies für die Telekommunikationsüberwachung bereits geschehen ist: Die Diensteanbieter müssen die zu überwachende Telekommunikation den Sicherheitsbehörden unverschlüsselt an einem Übergabepunkt bereitstellen.[1122]

Zusammenfassend können also die vier folgenden verschiedenen Optionen innerhalb des Szenario 2 unterschieden werden:[1123]

Unterszenario 2a
Staat S gestattet nur die Nutzung schwacher Verschlüsselungsverfahren bzw. die Verwendung kurzer Schlüssellängen.[1124]

Unterszenario 2b
Staat S gestattet nur die Nutzung von Verschlüsselungsverfahren mit einer technischen „Hintertür" (`*backdoor´*).

Unterszenario 2c
Staat S gestattet nur die Nutzung von Verschlüsselungsverfahren, bei denen die Schlüssel hinterlegt werden (`*key escrow´* oder `*key escrowing´*).[1125]

1121 Dies schient aber nach *Bizer*, Nachfrage nach Sicherheit, Privater Vertraulichkeitsschutz und staatliche Sicherheitspolitik in der Telekommunikation, in: *Bizer/Koch,* Sicherheit, Vielfalt, Solidarität, S. 29, 37 kein von den staatlichen Sicherheitsbehörden favorisiertes Modell zu sein: „Um bei der Durchführung von Überwachungsmaßnahmen die Abhängigkeit von den Betreibern zu minimieren, sieht sich der Staat nunmehr veranlaßt, den Sicherheitsbehörden einen möglichst *direkten Durchgriff* ohne Mitwirkung der Dienstebetreiber auf Inhalt und Umstände der Telekommunikation zu sichern."

1122 Vgl. § 8 Telekommunikations-Überwachungsverordnung (TKÜV) vom 03.11.2005 (BGBl. I 3136): „(3) Wenn der Verpflichtete die ihm zur Übermittlung anvertraute Telekommunikation netzseitig durch technische Maßnahmen gegen unbefugte Kenntnisnahme schützt, hat er die von ihm für diese Telekommunikation angewendeten Schutzvorkehrungen bei der an dem Übergabepunkt bereitzustellenden Überwachungskopie aufzuheben."

1123 Siehe eine umfangreiche Darstellung der denkbaren Optionen bei *Koops*, The crypto controversy, S. 143 ff. Zu den in Deutschland im Rahmen der Kryptokontroverse diskutierten Varianten siehe Schulzki-Haddouti, TP: Kanthers Kurs auf das Kryptoverbot, verfügbar unter: htt p://www.heise.de/tp/r4/artikel/1/1146/2.html (1.12.2008). Die dort vorgestellten Varianten basieren alle auf einem `*key escrow´*-Modell wie im Unterszenario 2c. Die diskutierten Varianten unterscheiden sich vor allem darin, wie stark die Möglichkeit der Nutzung anderer Verschlüsselungsverfahren neben solchen mit hinterlegten Schlüsseln beschränkt wird. Das hier diskutierte Szenario entspricht der Variante 3 bei *Schulzki-Haddouti*, bei der alle anderen Verfahren verboten werden. Die anderen Varianten greifen zwar weniger stark in Grundrechte ein, da die Nutzung anderer Verfahren möglich bleibt. Gleichzeitig wird dadurch aber auch die Erreichung des verfolgten Zwecks so unterminiert, dass die Regelungen deswegen starken verfassungsrechtlichen Bedenken unterliegen.

1124 So etwa die Rechtslage in Frankreich von 1998 bis zu einer weitergehenden Liberalisierung im Jahr 1999; vgl. Koops, Crypto Law Survey (Stand 01.07.2008), verfügbar unter: http://rec hten.uvt.nl/koops/cryptolaw/cls2. htm (23.10.2009).

Unterszenario 2d
Staat S gestattet nur die Nutzung von Verschlüsselungsverfahren, bei denen ein Nachschlüssel erzeugt werden kann (`*key recovery*´).

Die genannten Optionen werden hier alle zusammen als relative Verschlüsselungsverbote diskutiert, da sie alle auf dem Konzept basieren, dass einige Verschlüsselungsverfahren, die – auf unterschiedliche technisch-organisatorische Weise – die Kenntnisnahmemöglichkeiten der Sicherheitsbehörden garantieren, genutzt werden dürfen, alle übrigen Verschlüsselungsverfahren aber verboten werden.

Aus diesem Verbot aller übrigen Verschlüsselungsverfahren ergeben sich bedeutende Parallelen zu einem absoluten Verschlüsselungsverbot. Dementsprechend wird die folgende Prüfung der Verfassungsmäßigkeit eines relativen Verschlüsselungsverbots parallel zur Prüfung der Verfassungsmäßigkeit eines absoluten Verschlüsselungsverbots aufgebaut. Ausführlich erörtert werden dabei im Wesentlichen solche Aspekte, bei denen sich Abweichungen der rechtlichen Bewertung oder der zu Grunde liegenden Argumentation ergeben. Im Übrigen wird auf die Darstellung im Rahmen der Verfassungsmäßigkeit eines absoluten Verschlüsselungsverbots verwiesen. Im Ergebnis wird die rechtliche Bewertung eines relativen Verschlüsselungsverbots ohnehin entscheidend von der dargestellten Verfassungswidrigkeit eines absoluten Verschlüsselungsverbots geprägt.

A. Verschlüsselungsverbot und Privatsphärenschutz

I. Verstoß gegen das Fernmeldegeheimnis (Art. 10 I GG)

1. Schutzbereich des Fernmeldegeheimnisses (Art. 10 I GG)

Das Fernmeldegeheimnis gewährleistet ein Recht auf Verschlüsselung (s.o. in Teil 3 unter A.I.1.b.). Der Schutzbereich ist eröffnet.

2. Grundrechtseingriff durch ein relatives Verschlüsselungsverbot

Ein relatives Verschlüsselungsverbot würde in dieses Recht eingreifen. Zwar verbleiben dem Grundrechtsberechtigten Verschlüsselungsverfahren, die er legal nutzen kann, diese schützen aber gerade nicht vor der Kenntnisnahme staatlicher Sicherheitsbehörden. Grundsätzlich werden staatliche Einblicke in die vertrauliche Kom-

1125 Unter dieses Szenario fällt sowohl die Alternative, dass der Nutzer zur Hinterlegung verpflichtet ist (bei teilnehmerautonomer Verschlüsselung), wie die Variante, dass die Dienstanbieter Schlüsselduplikate aufbewahren müssen (bei Verschlüsselung durch den Dienstanbieter).

munikation ermöglicht.[1126] Gerade davor soll das Fernmeldegeheimnis aber schützen.[1127] Schließlich führen einige der diskutierten Optionen auch zu massiven Sicherheitseinbußen gegenüber sonstigen Angriffen interessierter Dritter:

- Bei der alleinigen Zulassung schwacher Verschlüsselungsverfahren oder kurzer Schlüssellängen, die eine erfolgreiche *`Brute-Force´*-Attacke der Sicherheitsbehörden ermöglichen würden (Unterszenario 2a), eröffnet dies auch für andere Interessierte mit vergleichbaren Ressourcen die Möglichkeit, die Verschlüsselung zu knacken. Sowohl im Bereich der Organisierten Kriminalität als selbstverständlich auch bei ausländischen Sicherheitsbehörden liegen sowohl das entsprechende Know-how als auch die technischen Ressourcen vor. Ein Schutz bestünde nur gegenüber einfachen Abhörversuchen sowie gegen zufällige Kenntnisnahme.[1128]

  „Größer noch wären die Akzeptanzprobleme bei Verfahren mit von vornherein – etwa durch Wahl der Schlüssellänge – begrenztem Sicherheitsniveau, zumal diese unter dem Makel leiden, auch nicht autorisierte Dritte dazu einzuladen, sich – entsprechende Kenntnis vorausgesetzt – nach Belieben zu `bedienen´."[1129]

- Bei Implementierung einer Hintertür (Unterszenario 2b), kann diese ebenfalls durch andere Interessierte genutzt werden. Hacker werden sich gezielt auf die Suche nach der Hintertür machen und die Erkenntnisse an die entsprechenden Kreise verkaufen – wie dies jetzt schon mit *`Less-Than-Zero-Day Exploits´* geschieht.
- Je nach technisch-organisatorischer Ausgestaltung sind auch bei den Unterszenarien 2c und 2d Angriffe auf die technische Infrastruktur, die zur Verwaltung der Schlüssel bzw. zur Erzeugung der Nachschlüssel benötigt wird, denkbar.[1130] Grundsätzlich ist dem bereits in der Kryptokontroverse Mitte der Neunziger Jahre vom damaligen Bundesforschungsminister Jürgen Rüttgers (CDU) vorgebrachten Argument Rechnung zu tragen:

  „So zeigt die Erfahrung, daß jede Abhörmöglichkeit für öffentliche Stellen innerhalb kurzer Zeit auch von nichtautorisierten Personen genutzt werden kann."[1131]

Ein relatives Verschlüsselungsverbot stellt somit einen Eingriff in das Fernmeldegeheimnis (Art. 10 I GG) dar.

1126 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 209 f.
1127 BVerfG, Urteil vom 02.03.2006, Az.: 2 BvR 2099/04, Rn. 65.
1128 *Hamm,* DuD 1997, 186, 188
1129 *Heuser*, Verschlüsselung im Spannungsfeld von staatlichem Anspruch und individueller Freiheit, in: *Kubicek,* Multimedia – Technik sucht Anwendung, S. 224, 226.
1130 Da keine konkreten derartigen Szenarien entwickelt wurden, wären weitere Überlegungen, welche Sicherheitsmaßnahmen und welche Angriffe darauf denkbar wären, reine Spekulation. Insoweit müssen hier generellere Aussagen ausreichen.
1131 *Rüttgers,* CR 1996, 51 53, der daraus ableitet, dass eine Abhörmöglichkeit im Zweifel nicht eingeführt werden sollte.

3. Verfassungsrechtliche Rechtfertigung eines relativen Verschlüsselungsverbots

a. Gesetzesvorbehalt

Die Einführung eines relativen Verschlüsselungsverbots wäre durch oder auf Grund eines Gesetzes möglich (s.o. in Teil 3 unter A.I.3.a.).

b. Verstoß gegen die Wesensgehaltsgarantie (Art. 19 II GG)

Ein solches relatives Verschlüsselungsverbotsgesetz könnte gegen die Wesensgehaltsgarantie (Art. 19 II GG) verstoßen:[1132]

- Für eine Antastung des Wesensgehalts des Fernmeldegeheimnisses durch ein relatives Verschlüsselungsverbotsgesetz spricht, dass auch ein relatives Verschlüsselungsverbot einen *Widerspruch zur Ideengeschichte des Fernmeldegeheimnisses* bedeuten würde (s.o. in Teil 3 unter A.I.3.b.cc)(1)). Auch ein relatives Verschlüsselungsverbot würde den effektiven Selbstschutz des Grundrechtsberechtigten untersagen zu Gunsten der Erhaltung staatlicher Kenntnisnahmeoptionen (vor denen Art. 10 I GG ja gerade schützen will).
- Für eine Antastung des Wesensgehalts spricht weiter, dass auch ein relatives Verschlüsselungsverbotsgesetz eine *Umkehrung der verfassungsrechtlichen Grundsatzwertungen* bedeuten würde (s.o. in Teil 3 unter A.I.3.b.cc)(2)). Ein relatives Verschlüsselungsverbot bedeutet nichts anderes als ein Verbot aller Verschlüsselungsverfahren, die effektiven individuellen Selbstschutz ermöglichen – nur Verfahren, die letztlich gegenüber dem Staat (und Dritten) keinen Schutz gewähren, werden zugelassen. Daher gilt auch für ein relatives Verschlüsselungsverbot, dass es effektiven individuellen Selbstschutz und damit grundrechtliche Freiheitsausübung grundsätzlich als „verdächtig" diskreditieren und rechtfertigungsbedürftig machen würde. Statt des Eingriffs in die grundrechtliche Freiheit wird so die Ausübung dieser Freiheit rechtfertigungsbedürftig:

  „Auch das Lizenzierungsmodell in Verbindung mit der Zulassung bestimmter Verschlüsselungsverfahren ist mit dem Makel belastet, die Ausübung des Fernmeldegeheimnisses in eine vorbeugende Offenbarungspflicht zu verkehren: Das Fernmeldegeheimnis wäre zwar durch staatliche lizenzierte Kryptoverfahren prinzipiell gegen Zugriff Dritter geschützt, aber um den Preis der prinzipiellen Zugriffsmöglichkeit der staatlichen Sicherheitsbehörden, gegen das es doch `historisch und aktuell´ schützen soll."[1133]

- Gegen eine Antastung des grundrechtlichen Wesensgehalts spricht aber, dass bei Erlass eines relativen Verschlüsselungsverbotsgesetzes *traditionelle, vor allem rechtliche Schutzmöglichkeiten erhalten* bleiben (s.o. in Teil 3 unter A.I.3.b.cc)(3)).

1132 Allgemein zur Wesensgehaltsgarantie sowie zur Annahme eines Verstoßes gegen die Wesensgehaltsgarantie durch ein absolutes Verschlüsselungsverbot s.o. in Teil 3 unter A.I.3.b.

1133 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 210.

- Gegen eine Antastung des Wesensgehalts spricht schließlich weiter, dass ein relatives Verschlüsselungsverbot neben den rechtlichen Schutzmöglichkeiten auch unmittelbaren, technischen Selbstschutz ermöglicht. Je nachdem welche Verschlüsselungsverfahren zugelassen werden (Unterszenarien 2a-2d), können diese technischen Optionen durchaus ein *gegenüber nicht-staatlichen Dritten hohes Sicherheitsniveau* gewährleisten (so etwa für die Unterszenarien 2c und 2d).
- Werden dagegen nur schwache Verschlüsselungsverfahren bzw. kurze Schlüssellängen (Unterszenario 2a) zugelassen oder Verfahren mit einer technischen Hintertür (Unterszenario 2b), gewährleisten diese Verfahren ein so geringes Sicherheitsniveau, dass nahezu jeder Interessierte Kommunikation mitlesen und überwachen könnte. Ein derart *unzureichender tatsächlicher Schutz* spricht – auch bei fortbestehendem rechtlichen Schutz – für die Annahme eines Verstoßes gegen die Wesensgehaltsgarantie des Fernmeldegeheimnisses (s.o. in Teil 3 unter A.I.3.b.cc)(4)).
- Für eine Antastung des grundrechtlichen Wesensgehalts spricht zuletzt auch die Betroffenheit von Inhalten, die zum *unantastbaren Kernbereich privater Lebensgestaltung* gehören (s.o. in Teil 3 unter A.I.3.b.cc)(5)). Verfahrensmäßige Vorkehrungen zum Kernbereichsschutz gegenüber nicht-staatlichen Akteuren sind auch bei einem relativen Verschlüsselungsverbotsgesetz nicht effektiv möglich.

Der in der Betroffenheit des unantastbaren Kernbereichs privater Lebensgestaltung liegende Verstoß gegen den Menschenwürdegehalt des Fernmeldegeheimnisses bedeutet zugleich einen Verstoß gegen den grundrechtlichen Wesensgehalt (Art. 19 II GG).[1134] Die zentralen Argumente, die bereits für ein absolutes Verschlüsselungsverbotsgesetz zu der Annahme eines Verstoßes gegen die Wesensgehaltsgarantie geführt haben, gelten genauso für ein relatives Verschlüsselungsverbot. Einzig die Varianten eines relativen Verschlüsselungsverbotsgesetzes, die ein hohes Sicherheitsniveau gegenüber nicht-staatlichen Dritten gewährleisten (Unterszenarien 2c und 2d), erfahren eine leicht abweichende Beurteilung, da sie immerhin einen gewissen technischen Selbstschutz des Fernmeldegeheimnisses gestatten. Angesichts des fehlenden Schutzes gegenüber staatlichen Stellen, der Umkehrung verfassungsrechtlicher Grundsatzwertungen und der Betroffenheit des grundrechtlichen Menschenwürdegehalts kann dies aber an der Annahme eines Verstoßes gegen die Wesensgehaltsgarantie (Art. 19 II GG) nichts ändern. Auch ein relatives Verschlüsselungsverbotsgesetz würde folglich den grundrechtlichen Wesensgehalt des Fernmeldegeheimnisses sowie den Menschenwürdegehalt antasten – unabhängig davon, welches Unterszenario betrachtet wird. Da Literatur und Rechtsprechung nur selten einen Verstoß gegen die Wesensgehaltsgarantie annehmen, wird im Weiteren noch die Verhältnismäßigkeit eines relativen Verschlüsselungsverbotsgesetzes untersucht:

1134 Ausführlich zum Zusammenhang von Kernbereichsschutz, Menschenwürde- und Wesensgehalt oben in Teil 3 unter A.I.3.b.cc)(5).

c. Verhältnismäßigkeitsgrundsatz

aa) Legitimer Zweck

Ein relatives Verschlüsselungsverbotsgesetz dient den legitimen Zwecken der Verfolgung und Verhütung von Straftaten sowie der Sicherung des Rechtsfriedens (s.o. in Teil 3 unter A.I.3.c. aa)).

bb) Geeignetheit

Ein relatives Verschlüsselungsverbotsgesetz müsste weiter geeignet sein, diese Zwecke zu fördern. Dies ist – wie auch bei einem absoluten Verschlüsselungsverbot (s.o. in Teil 3 unter A.I.3.c.bb)) - äußerst zweifelhaft: [1135]

(1) Noch effektivere Umgehungsmöglichkeiten

Aus der Tatsache, dass manche Verschlüsselungsverfahren genutzt werden dürfen, andere hingegen nicht, ergeben sich noch mehr und noch effektivere Möglichkeiten, ein Verschlüsselungsverbot zu umgehen.[1136] Eine Nachricht, die vertraulich übermittelt werden soll, kann erst mit einem illegalen, aber abhörsicheren Verschlüsselungsverfahren verschlüsselt werden und dieser Chiffretext kann im Anschluss nochmal verschlüsselt werden – mit einem zugelassenen Verfahren (sog. „Überschlüsseln“).[1137] Ein „Verstecken“ (s.o. in Teil 3 unter A.I.3.c.bb)(4)) verschlüsselter Nachrichten wäre gar nicht mehr erforderlich, da die Nachricht mit einem zugelassenen Verschlüsselungsverfahren verschlüsselt zu sein scheint.

> „Diejenigen, die den Inhalt ihrer Gespräche für kriminelle Zwecke geheimhalten wollen, werden zu anderen Methoden greifen, speziell zu Verfahren der „Überschlüsselung“ von Nachrichten mit einem legalen Schlüssel. die zuvor mit einem illegalen (nichtbrechbaren) Algorithmus verschlüsselt wurden.“[1138]

1135 *Koch,* CR 1997, 106, 108 f.; *Bizer*, Verschlüsselung und staatlicher Datenzugriff, in: *Büllesbach,* Datenschutz im Telekommunikationsrecht, S. 245, 263 ff.; *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 205 ff.; *Meyn*, Verschlüsselung und Innere Sicherheit, S. 104 ff.

1136 Siehe allgemein zu den Umgehungsmöglichkeiten oben in Teil 3 unter A.I.3.c.bb)(1).

1137 Vgl. *Hamm,* DuD 1997, 186, 189; zu den Einzelheiten der Vorgehensweise siehe *Huhn/Pfitzmann,* DSB 1996, 2, 4.

1138 *Dix,* CR 1997, 38, 42.

(2) Erhöhte Schwierigkeit der Feststellung von Umgehungsmaßnahmen

Bei einer Überschlüsselung wären Umgehungsmaßnahmen des relativen Verschlüsselungsverbotsgesetzes daher noch schwieriger feststellbar.[1139] Wirklich feststellen könnten die Sicherheitsbehörden den Einsatz nicht lizenzierter Verschlüsselungsverfahren erst, wenn ihnen eine Überwachungsanordnung die Entschlüsselung der betreffenden Kommunikation gestatten würde. Erst dann könnte überhaupt der Verdacht entstehen, dass es sich bei den für die Sicherheitsbehörden nicht entzifferbaren Daten um eine weitere Verschlüsselung handeln könnte.[1140]

(3) Fortbestehende Kontrollprobleme

Die Problematik der Etablierung effektiver Kontrollbefugnisse hinsichtlich der Einhaltung des Verschlüsselungsverbots besteht in gleicher Weise wie bei einem absoluten Verschlüsselungsverbotsgesetz fort (s.o. in Teil 3 unter A.I.3.c.bb)(3)). Effektive Kontrolle wäre nur bei einer möglichst verdachtsunabhängigen Kontrolle zu erreichen. Dies wäre aber ein klarer Verstoß gegen das Fernmeldegeheimnis und verstieße nach einer in der Literatur vertretenen Auffassung sogar gegen die Wesensgehaltsgarantie:

> „Überdies müßte eine immense Überwachungsbürokratie geschaffen werden, die jede (auch unverdächtige) Telekommunikationsverbindung auf die mögliche Verwendung illegaler Verschlüsselungsverfahren hin überprüfen müßte. Damit wäre die Garantie des Fernmeldegeheimnisses in ihrem Wesensgehalt (Art. 19 Abs. 2 GG) angetastet."[1141]

(4) Ergebnis

Auch wenn die Umgehungsmöglichkeiten mit einem relativen Verschlüsselungsverbotsgesetz eher noch einfacher werden und die übrigen Probleme bei der Umsetzung eines Verschlüsselungsverbots fortbestehen, könnte man im Hinblick auf den weiten Einschätzungsspielraum des Gesetzgebers ein relatives Verschlüsselungsverbot (noch) für geeignet halten (s.o. in Teil 3 unter A.I.3.c.bb)(9)).

cc) Erforderlichkeit

Die unmittelbare Zielsetzung eines relativen Verschlüsselungsverbots, die Nutzung von Verschlüsselungsverfahren, die eine staatliche Kenntnisnahme verhindern wür-

1139 Vgl. zu den Schwierigkeiten bei der Feststellung von Umgehungen oben in Teil 3 unter A.I.3.c.bb)(2).

1140 Es wurde bereits darauf hingewiesen, dass es sich aber ebenso gut um ein Computerprogramm, eine komprimierte Datei oder Datenschrott handeln könnte.

1141 *Dix,* CR 1997, 38, 42.

den, zu unterbinden, kann nicht durch ein anderes Mittel erreicht werden (s.o. in Teil 3 unter A.I.3.c.cc)). Ein relatives Verschlüsselungsverbotsgesetz wäre daher erforderlich.

dd) Verhältnismäßigkeit im engeren Sinne

Bei der Abwägungsentscheidung im Rahmen der Verhältnismäßigkeit im engeren Sinn ergeben sich zunächst keine gravierenden Abweichungen zwischen relativem und absolutem Verschlüsselungsverbotsgesetz (s.o. in Teil 3 unter A.I.c.dd)):

- Da alle von einem relativen Verschlüsselungsverbot betroffen wären, bleibt es bei der festgestellten *größtmöglichen Streubreite* des Eingriffs.
- Die *Eingriffsqualität* ist allerdings teilweise *geringer*, da immerhin ein Schutz gegen technisch wenig versierte oder wenig ressourcenstarke Angreifer sowie gegen zufällige Kenntnisnahme möglich ist. Je nachdem, welche Verschlüsselungsverfahren im Einzelnen zugelassen werden, beurteilt sich entsprechend die Angriffssicherheit. Bei der Zulassung nur schwacher Verfahren oder kurzer Schlüssellängen sowie bei Implementierung einer Hintertür (Unterszenarien 2a und 2b) bestehen gravierende Angriffsmöglichkeiten, so dass die Eingriffsqualität kaum verringert wird. Die Schlüsselhinterlegungsmodelle oder Nachschlüsselmodelle (Unterszenarien 2c und 2d) dürften dagegen ein hohes Sicherheitsniveau gegenüber Angriffen interessierter Dritter gewährleisten.[1142] Für diese Modelle ist die Eingriffsqualität geringer als bei einem absoluten Verschlüsselungsverbot.
- Gleichwohl bleiben die *Einschüchterungseffekte*, die aus dem Bewusstsein einer möglichen Kommunikationsüberwachung resultieren, erhalten:

  „Aus Sicht der Grundrechtsträger führt das Lizensierungsmodell zu einer prinzipiellen Verunsicherung der aktuellen Kommunikationssituation."[1143]

- Allerdings dient ein relatives Verschlüsselungsverbotsgesetz der *Wahrnehmung gewichtiger Allgemeinwohlbelange*.
- Ein relatives Verschlüsselungsverbotsgesetz würde dagegen *noch mehr Umgehungsmöglichkeiten* schaffen, insbesondere könnte sich jeder den Schein normgerechten Verhaltens geben, indem er ein mit einem illegalen Verschlüsselungsverfahren erstelltes Chiffrat nochmals verschlüsselt – diesmal mit einem staatlich zugelassenen Verfahren. Damit würde im Regelfall der Einsatz nicht zugelassener Verschlüsselungsverfahren erst entdeckt werden, wenn aufgrund einer Überwachungsanordnung die Kommunikation entschlüsselt würde.
- Die *Effizienz der Überwachungsmaßnahmen*, die durch ein relatives Verschlüsselungsverbotsgesetz aufrecht erhalten werden sollen, ist ungewiss.

1142 So die Einschätzung von *Hamm,* DuD 1997, 186, 188 für `*key escrowing*´-Verfahren.
1143 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 211.

Unter Berücksichtigung dieser Aspekte dürfte sich am ehesten ein Schlüsselhinterlegungsmodell oder ein Nachschlüsselmodell als verhältnismäßig erweisen, da den zunehmenden Umgehungsmöglichkeiten wenigstens ein echter Sicherheitszuwachs der Nutzer für ihre Daten gegenüber Angriffen nicht-staatlicher Dritter gegenübersteht. Allerdings müssten sowohl bei einem Hinterlegungs- als auch einem Nachschlüsselmodell Informationen bei einer staatlichen oder privaten Stelle gespeichert sein: Entweder ist der verwendete Schlüssel dort zu hinterlegen (Schlüsselhinterlegungsmodell) oder es sind zusätzliche Informationen zu hinterlegen, aus denen sich dann bei Bedarf der Nachschlüssel generieren lässt (Nachschlüsselmodell)[1144]. Insoweit nähern sich die Unterszenarien 2c und 2d in ihrer rechtlichen Bewertung stark an. Insbesondere sind folgende weitere Aspekte im Rahmen der Verhältnismäßigkeit im engeren Sinne zu berücksichtigen:

(1) Neue Angriffsszenarien auf die Infrastruktur

Da somit sowohl ein Nachschlüssel- als auch ein Hinterlegungsmodell auf eine technisch-organisatorische Infrastruktur[1145] zur sicheren Verwaltung und Aufbewahrung der Schlüsselduplikate bzw. der zur Nachschlüsselerzeugung erforderlichen

1144 Würde sich alle Information zur Generierung des Nachschlüssels aus den verschlüsselten Daten selbst ergeben, würde es sich in der Sache um nichts anderes als eine Hintertür handeln, die auch jeder sonstige interessierte Dritte mit dem entsprechenden Know-how ausnutzen könnte. Ein hohes Sicherheitsniveau könnte nur Nachschlüsselmodellen attestiert werden, die allein mit zusätzlichen, an anderer Stelle hinterlegten Informationen die Generierung des Nachschlüssels gestatten.

1145 Vgl. umfassend zum Infrastrukturbegriff bei Kommunikationsinfrastrukturen *Hermes*, Staatliche Infrastrukturverantwortung, S. 164 ff. sowie jüngst unter dem Schlagwort eDaseinsvorsorge *Luch/Schulz,* MMR 2009, 19. Zur Übertragbarkeit des Infrastrukturbegriffs auf technische Systeme wie Verschlüsselung siehe *Hammer*, Gestaltungsbedarf und Gestaltungsoptionen für Sicherungsinfrastrukturen, in: *Hammer,* Sicherungsinfrastrukturen, S. 41, 42 ff. Unabhängig davon, ob man den Staat selbst im Rahmen der Daseinsvorsorge verpflichtet sieht oder die Schaffung rechtlicher Rahmenbedingungen für eine durch Private umzusetzende Infrastruktur für ausreichend hält, scheint jedenfalls Einigkeit zu herrschen, dass Vertraulichkeit und Integrität als Kernelemente von IT-Sicherheit einer Infrastruktur bedürfen. So jedenfalls bereits *Hammer*, Gestaltungsbedarf und Gestaltungsoptionen für Sicherungsinfrastrukturen, in: *Hammer,* Sicherungsinfrastrukturen, S. 41, 44 sowie jüngst Bundesministerium des Innern, Bürgerportale, verfügbar unter: http://www.kbst.bund.de/cln_028/nn_1100856/SharedDocs/Anlagen-kbst/Bportale/bportal-ueberblick-V0-96.pdf,templateId=raw,property=publicationFile.pdf/bportal-ueberblick-V0-96.pdf (19.09.2008), S. 3: „Der moderne Staat steht deshalb heute vor der Aufgabe, im elektronischen Kommunikationsraum für eine Grundversorgung an Sicherheit, Verbindlichkeit und Vertraulichkeit zu sorgen. Staatliche Regulierung kann und muss jedoch nicht bedeuten, selbst eine Infrastruktur aufzubauen und Dienste der Allgemeinheit anzubieten. Sie kann sich, sofern dies für die Sicherung der Grundversorgung ausreicht, darauf beschränken, Regeln zu definieren und ihre Einhaltung zu kontrollieren, wenn es darum geht, das Angebot und die Sicherheit dieser wesentlichen Dienste und ihre Nutzbarkeit für alle zu gewährleisten."

Zusatzinformationen angewiesen sind, ergeben sich neue Angriffsszenarien auf diese Infrastruktur:

> „Um dieses System zu verwalten, bedarf es einer riesigen Infrastruktur. Die Regierungsbehörden müssen Produkte, Leistungen und Trust Centers überprüfen und zertifizieren. Andere Behörden werden diese Tätigkeit koordinieren. Ein Sicherheitsleck an einer Stelle dieser Struktur kann zur Kompromittierung vieler Schlüssel und damit zu großen Schäden führen."[1146]

Zwar ist das eingesetzte Verschlüsselungsverfahren an sich sicher. Die Aufbewahrung von Schlüsselduplikaten bzw. Nachschlüsselinformationen schafft aber neue Angriffsrisiken. Die Aufbewahrungsinstanzen werden zur „höchst sicherheitsempfindlichen Stellen".[1147] Neben der hohen technisch-organisatorischen Sicherheit, die derartige Stellen gewährleisten müssten, scheitert die Erreichung absoluter Sicherheit allein schon wegen des Vorhandenseins der „Fehlerquelle Mensch". Neben menschlichen Fehlern bei der Implementierung und Umsetzung von (IT-)Sicherheitsmaßnahmen ist insbesondere an *`Social Engineering´*-Angriffe und den „beträchtlichen Bestechungsdruck"[1148] zu denken.

Derartige Infrastrukturangriffe sind zwar äußerst schwierig umzusetzen, gleichwohl stellen sie angesichts der Interessen und Ressourcen sowohl im Bereich der Organisierten Kriminalität wie von Seiten ausländischer Geheimdienste realistische Szenarien dar. Die Schäden, die bei einem Sicherheitsleck innerhalb der gewaltigen Sicherungsinfrastruktur auftreten können, sind enorm.[1149]

(2) Keine korrespondierenden Vorteile für den Nutzer

Zum Teil wurde argumentiert, dass eine Hinterlegung von Schlüsselduplikaten bzw. Nachschlüsselinformationen auch dem Nutzer Vorteile bringen würde:[1150] Der Nutzer sei so davor geschützt, dass bei Verlust des Schlüssels seine eigenen Daten für ihn unentschlüsselbar und damit unbrauchbar werden. Davor kann ihn aber letztlich auch eine Speicherung von Schlüsselduplikaten oder Nachschlüsselinformationen nicht schützen:

1146 *Andrzejak*, Kryptoregulierung, in: *Hoeren/Queck,* Rechtsfragen der Informationsgesellschaft, S. 132, 143.

1147 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 210. Das Sicherheitskonzept für die Aufbewahrung der Schlüssel zum Signieren der Rootzone des *`Domian Name Systems´* (DNS) für die Einführung des neuen Protokolls DNSSEC (*`DNS Security Extensions´*) kann insoweit einen Eindruck vermitteln: heise online vom 11.11.2009, DNS: Sieben Schlüsselbewahrer für die Rootzone, verfügbar unter: http://www.heise.de/newsticker/meldung/DNS-Sieben-Schluesselbewahrer-fuer-die-Rootzone-856563.html (12.11.2009).

1148 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 210; *Hamm,* DuD 1997, 186, 188 nennt daneben auch noch Erpressung als besonderes Risiko.

1149 *Andrzejak*, Kryptoregulierung, in: *Hoeren/Queck,* Rechtsfragen der Informationsgesellschaft, S. 132, 143.

1150 Siehe dazu Huhn/Pfitzmann, Technische Randbedingungen jeder Kryptoregulierung, verfügbar unter: http://events.ccc.de/congress/1995/div/pfitz/krypto.htm (18.12.2006).

- Tatsächlich ist eine Schlüsselsicherung (häufig auch Schlüsselbackup genannt) für den Fall des Verlustes seines Schlüssels nur dann notwendig, wenn es sich um *verschlüsselte eigene Daten jenseits von Kommunikationsprozessen* handelt (etwa das verschlüsselte elektronische Tagebuch auf dem eigenen Rechner oder die verschlüsselte Festplatte). Denn diese Daten wären tatsächlich „verloren", wenn eine Entschlüsselung bei Verlust des Schlüssels nicht mehr möglich wäre. Diese Schlüssel zur Verschlüsselung der eigenen Daten auf dem eigenen Rechner sind aber nicht Gegenstand eines Schlüsselhinterlegungs- oder Nachschlüsselmodells, welches immer an Kommunikationsprozesse anknüpft.
- Geht es dagegen um *verschlüsselte Kommunikation*, sind die Daten beim jeweils anderen Kommunikationspartner noch vorhanden. Es ist daher gar nicht zwingend erforderlich, die mit dem verlorenen Schlüssel verschlüsselten Daten zu entschlüsseln. Es ist sicherer und (zumeist) auch einfacher, sich die Daten mit einem neuen Schlüssel verschlüsselt nochmals senden zu lassen, anstatt auf eine Schlüsselsicherungsinfrastruktur zurückzugreifen – welche immer neue Angriffspunkte schafft.[1151]
- In jedem Fall sollten Schlüssel zur verschlüsselten Kommunikation niemals auch zur Verschlüsselung eigener Daten jenseits von Kommunikation benutzt werden. Unterschiedliche Funktionalitäten (sichere Kommunikation einerseits, sichere Datenaufbewahrung andererseits) sollten zur Erhöhung der Sicherheit stets von unterschiedlichen Schlüsseln erbracht werden.[1152] Hält sich der Nutzer an diese elementare Sicherheitsregel, können ihm gerade in den Fällen, in denen tatsächlich ein Datenverlust droht (nämlich bei Verlust des Schlüssels für die eigene Datensicherung), auch staatlich gespeicherte Schlüsselduplikate bzw. Nachschlüsselinformationen nicht helfen, da diese nur für Schlüssel, die zur Kommunikation verwendet wurden, vorliegen – also für Daten, die regelmäßig auch anderweitig wieder beschafft werden können.

Zur Sicherung der wirklich sicherungsbedürftigen Schlüssel (nämlich denen zur privaten Datensicherung) kann ein Schlüsselhinterlegungs- oder Nachschlüsselmodell somit nichts beitragen.

Daneben wurde auch vorgebracht, eine solche Schlüsselhinterlegungs- oder Nachschlüsselinfrastruktur löse das sog. Zertifizierungsproblem, d.h. die Frage der (rechts-)sicheren Zuordnung eines Schlüssels zu einer Person: Schlüssel zur vertraulichen Kommunikation benötigen aber – im Gegensatz zur digitalen Signatur – keinerlei Zertifizierung einer offiziellen Zertifizierungsstelle, entscheidend ist allein, *dass* die Authentizität festgestellt wird.[1153] Bei der elektronischen Signatur muss der Schlüssel in rechtlich nachweisbarer Weise einer bestimmten Person zuzuordnen

1151 Huhn/Pfitzmann, Technische Randbedingungen jeder Kryptoregulierung, verfügbar unter: htt p://events.ccc. de/congress/1995/div/pfitz/krypto.htm (18.12.2006).

1152 *Huhn/Pfitzmann,* DSB 1996, 2, 3.

1153 *Huhn/Pfitzmann,* DSB 1996, 2, 2 sowie Huhn/Pfitzmann, Technische Randbedingungen jeder Kryptoregulierung, verfügbar unter: http://events.ccc.de/congress/1995/div/pfitz/krypto.htm (18.12.2006).

sein – hierfür wird die Zertifizierung durch eine anerkannte Zertifizierungsstelle benötigt. Für vertrauliche Kommunikation reicht es dagegen aus, wenn die *Kommunikationspartner* wissen, dass sie den korrekten Schlüssel ihres Kommunikationspartners haben – auf eine *rechtliche* Nachweisbarkeit kommt es in keiner Weise an. Daher reicht etwa ein persönlicher Schlüsseltausch für Zwecke der vertraulichen Kommunikation völlig aus. Eine offiziell anerkannte Zertifizierung ist dazu nicht erforderlich.

Zusammenfassend kann festgestellt werden, dass eine Hinterlegung von Schlüsseln oder Nachschlüsselinformationen für den Nutzer keinerlei spezifische Vorteile mit sich bringt.

(3) Sicherheitsbedenken hinsichtlich der digitalen Signatur

Schließlich ist besonderes Augenmerk auf die Tatsache zu richten, dass Verschlüsselungsverfahren nicht nur zur Verschlüsselung genutzt werden, sondern dass auch die digitale Signatur auf Verschlüsselungsverfahren basiert:[1154]

> „Die Kryptokontroverse um die Sicherheit vertraulicher Kommunikation wird durch die zusätzliche Funktion asymmetrischer Verschlüsselungsverfahren als Instrument rechtsverbindlicher Telekooperation verschärft."[1155]

Daraus ergeben sich folgende Konsequenzen:

- Die für die digitale Signatur eingesetzten Verschlüsselungsverfahren müssen ein extrem hohes Sicherheitsniveau gewährleisten:

  > „Die digitale Signatur ist als Sicherungsinstrument rechtsverbindlicher Telekooperation jedoch nur tauglich, wenn das hierzu verwendete öffentliche Schlüsselverfahren mathematisch sicher, technisch korrekt implementiert und die Sicherungsinfrastruktur integer und vertrauenswürdig ist."[1156]

- Im Hinblick auf den hohen Beweiswert, der qualifizierten elektronischen Signaturen[1157] zukommt,[1158] muss sichergestellt werden, dass nur der Berechtigte auf

1154 Diese Bedenken treffen grundsätzlich auch für ein absolutes Verschlüsselungsverbot zu. Hier wurde bei einem absoluten Verschlüsselungsverbot davon ausgegangen, dass tatsächlich alle Verschlüsselungsverfahren untersagt werden – mithin auch solche, die zum digitalen Signieren genutzt werden sollen. Wollte man bei einem absoluten Verschlüsselungsverbot nicht auf die digitale Signatur verzichten, würden sich dieselben Probleme ergeben wie hier für das relative Verschlüsselungsverbot dargestellt.

1155 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 212.

1156 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 212.

1157 „Elektronische Signatur" meint den Rechtsbegriff im Sinn von § 2 Nr. 1-3 SigG. „Digitale Signatur" ist der technische Begriff für das Verfahren, das der fortgeschrittenen wie der qualifizierten elektronischen Signatur (§ 2 Nr. 2, 3 SigG) zu Grunde liegt.

1158 Vgl. etwa § 371a ZPO i.d.F. vom 05.12.2005 (BGBl. I 3202): „[Beweiskraft elektronischer Dokumente] (1) Auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur

seinen Schlüssel zugreifen kann – weswegen dieser in der Regel unausforschbar auf einer Chipkarte gespeichert ist.[1159]

„Solange nicht ausgeschlossen werden kann, daß sich Dritte der Schlüssel zur Verfolgung ihrer Interessen bemächtigen können, so lange können diese Schlüssel auch nicht zur Sicherung rechtsverbindlicher Telekooperation verwendet werden."[1160]

Ein relatives Verschlüsselungsverbotsgesetz ist mit diesen Anforderungen nicht in Einklang zu bringen: Schwache Verfahren oder Verfahren mit Hintertür (Unterszenarien 2a und 2b) können nicht das erforderliche Sicherheitsniveau gewährleisten. Rechtssichere digitale Signaturen auf der Basis dieser Verschlüsselungsverfahren sind nicht denkbar, so dass bei diesen Szenarien auf digitale Signaturen verzichtet werden müsste.

Verfahren, bei denen die Schlüssel hinterlegt werden oder die Generierung von Nachschlüsseln möglich ist (Unterszenarien 2c und 2d), sind ebenfalls inkompatibel mit dem für eine digitale Signatur erforderlichen Sicherheitsniveau, da diese dem Erfordernis der strikten Gemeinhaltung der Signaturschlüssel nicht gerecht werden können. Einzige Lösung könnte die strikte organisatorische und technische Trennung der Schlüssel für die digitale Signatur einerseits und für die Verschlüsselung andererseits darstellen:

„Will man entgegen der oben näher ausgeführten verfassungsrechtlichen Bedenken nicht auf die Diskreditierung der Vertraulichkeit der Kommunikation verzichten, dann läßt sich der Schaden für eine im Streitfall erfolgreiche Beweisführung mit einem digital signierten Dokument nur beschränken, wenn eine technische und organisatorische Trennung der Schlüsselpaare zum Schutz der Vertraulichkeit einerseits und für Zwecke rechtsverbindlicher Telekooperation andererseits sichergestellt ist."[1161]

Da für die Vergabe und Zertifizierung digitaler Signaturen ohnehin bereits eine entsprechend Sicherungsinfrastruktur besteht, möchte man diese aber eigentlich auch für die Hinterlegung der Schlüsselduplikate bzw. der Informationen zur Erzeugung eines Nachschlüssels nutzen.[1162] Dies würde eine beweissichere digitale Signatur kompromittieren.

durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist."

1159 Vgl. ausführlich zu den Missbrauchsrisiken sowie zu den denkbaren Vertrauenseinbußen durch „digitale Legenden" für verdeckte Ermittler u.ä. ausführlich *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 213 f.: „Denkbar ist aber auch, daß im Zuge neuer Fahndungsmethoden wirkliche Rechtspersonen im elektronischen Rechtsverkehr simuliert werden sollen. Diese Variante setzt voraus, daß die Sicherheitsbehörden über Schlüsselduplikate der wirklichen Person verfügt, eine Voraussetzung, die einen kaum zu rechtfertigenden Eingriff in das Persönlichkeitsrecht der betroffenen Person darstellen würde und bereits als rechtlich legitimierte Möglichkeit geeignet ist, die Vertrauenswürdigkeit von Handlungen und damit den gesamten Rechtsverkehr zu zerstören."

1160 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 213.

1161 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 213.

1162 So war es laut *Andrzejak*, Kryptoregulierung, in: *Hoeren/Queck,* Rechtsfragen der Informationsgesellschaft, S. 132, 139 zumindest in der Kryptodebatte der Neunziger Jahre vorgesehen. Auch in den USA sollen die Trust Center, bei denen Schlüssel hinterlegt werden, auch die

(4) Sicherer Schlüsseltausch mit der digitalen Signatur

Auch wenn man die Sicherungsinfrastruktur für die digitale Signatur einerseits und ein Schlüsselhinterlegungs- oder Nachschlüsselmodell andererseits völlig trennen würde, hat die Zulässigkeit von digitalen Signaturen Bedeutung für Verfassungsmäßigkeit von relativen Verschlüsselungsverboten. Die digitale Signatur erlaubt einen vereinfachten authentischen Schlüsseltausch zur Durchführung von Verschlüsselung:

> „Jede Sicherheitsinfrastruktur für digitale Signaturen erlaubt den sicheren Austausch von Schlüsseln für Konzelation [Anm.: Synonym für Verschlüsselung]: Nach öffentlich bekannten Algorithmen mittels allgemein verfügbarer Programme kann jeder für Konzelation geeignete Schlüsselpaare generieren, seine öffentlichen Konzelationsschlüssel selbst zertifizieren, indem er eine Nachricht unterschreibt: "Der öffentliche Schlüssel ... gehört ...".“[1163]

Der neuralgische Punkt jeder verschlüsselten Kommunikation – der sichere Schlüsseltausch – wird also wesentlich vereinfacht, so dass auch einander unbekannte Personen mit etwas Vorarbeit vertraulich kommunizieren können. Die digitale Signatur löst eines der existenziellen Probleme, die einem Einsatz von Verschlüsselung entgegenstehen können (Die Schlüssel zur Nutzung illegaler Verschlüsselungsverfahren können ja weder über eine staatliche Infrastruktur noch über öffentliches Vertrauen etwa eines `*Web of trust*´ zertifiziert werden.). Sichere digitale Signatur und relatives Verschlüsselungsverbot sind daher nicht miteinander vereinbar.

(5) Sicherer Schlüsseltausch mit zugelassenen Verschlüsselungsverfahren

Schließlich kann auch jedes sichere Verschlüsselungsverfahren für einen sicheren Schlüsseltausch verwendet werden:

> „Ähnlich wie sichere digitale Signaturen zum sicheren Austausch von Schlüsseln für Konzelation verwendet werden können, kann auch jedes Konzelationssystem, also insbesondere auch jedes Key-Escrow-System, benutzt werden, um Schlüssel für zusätzliche zu verwendende Konzelationssysteme zu vereinbaren. Statt einem Konzelationssystem direkt die vertraulich zu haltenden Nachrichten zu übergeben, wird zunächst ein öffentlicher Konzelationsschlüssel redundant codiert übertragen. Der Empfänger prüft die Redundanz (was dem Prüfen des Zertifikates bei Verwendung digitaler Signaturen entspricht). Sofern er keine Verfälschung des öffentlichen Schlüssels feststellt, verwendet er den öffentlichen Schlüssel entweder, um wirklich vertraulich zu haltende Nachrichten zu verschlüsseln oder aber zum Austausch eines weiteren Schlüssels für ein symmetrisches Konzelationssystem, mit dem dann effizienter verschlüsselt werden kann. Bei der weiteren Kommunikation werden dann die mit dem aufgesetzten Konzelationssystem bereits verschlüsselten Nachrichten mit dem zugrundeliegenden Key-Escrow-Konzelationssystem ein weiteres Mal verschlüsselt.“[1164]

Schlüssel für eine digitale Signatur zertifizieren (*Andrzejak*, Kryptoregulierung, in: *Hoeren/Queck,* Rechtsfragen der Informationsgesellschaft, S. 132, 134).

1163 *Huhn/Pfitzmann,* DSB 1996, 2, 3.

1164 Huhn/Pfitzmann, Technische Randbedingungen jeder Kryptoregulierung, verfügbar unter: http://events.ccc.de/congress/1995/div/pfitz/krypto.htm (18.12.2006).

Als Fazit kann also festgehalten werden: *Existieren irgendwelche sicheren Verfahren (seien es Verfahren für die digitale Signatur oder seien es Verschlüsselungsverfahren, die bis auf die Zugriffsmöglichkeit des Staates via Schlüsselduplikat oder Nachschlüssel zunächst sicher sind), können diese immer dazu benutzt werden, ein Verschlüsselungsverbot auszuhebeln*. Die ohnehin bereits zweifelhafte Geeignetheit eines Verschlüsselungsverbots sinkt weiter.

(6) Dauerhafte Vertraulichkeitsgefährdung

Weiter ist im Rahmen der Verhältnismäßigkeit im engeren Sinne zu berücksichtigen, dass bei einem Hinterlegungs- wie bei einem Nachschlüsselmodell ein Zugriff auf die verwendeten Schlüssel eine *umfassende* Entschlüsselung ermöglicht:

> „Besondere Implikation dieses Verfahrens ist, daß der einmalige Zugriff auf die Schlüssel sowohl das Entschlüsseln vergangener als auch zukünftiger Verschlüsslungen ermöglicht."[1165]

(7) Ineffektive verfahrensrechtliche und organisatorische Sicherung des Schlüsselzugriffs

Allein deshalb ist eine verfahrensrechtliche und organisatorische Sicherung des Schlüsselzugriffs geboten. Derartige Sicherungsmaßnahmen, etwa ein Richtervorbehalt, können aber nur da funktionieren, wo die Voraussetzungen des Schlüsselzugriffs (etwa: besondere Schwere der Straftat, Aussichtslosigkeit anderer Ermittlungsinstrumente) überwacht werden. Ist der Schlüssel einmal zur Entschlüsselung freigegeben, kann jedenfalls ein Richter nicht mehr überwachen, welche Nachrichten damit entschlüsselt werden:

> „Zwar könnte der Zugriff auf die Schlüsselduplikate verfahrensrechtlich und organisatorisch durch eine richterliche Anordnung und öffentliche Berichts- und Rechtfertigungspflichten wie in den USA beschränkt werden, gleichwohl ist diese Sicherung unzureichend, wenn einmal kompromittierte Schlüssel technisch das Entschlüsseln aller vergangenen und zukünftigen Nachrichten an den Empfänger ermöglichen."[1166]

Dies birgt die Gefahr, dass Sicherheitsbehörden tatsächlich mehr entschlüsseln als durch die richterliche Kontrolle freigegeben wurde – bei dem Verdacht der Gefahr eines terroristischen Anschlags o.ä. sicher eine nahe liegende Befürchtung und allzu menschliche Verhaltensweise.[1167] Dies wird sicher begünstigt durch die Tatsache, dass dem deutschen Recht eine der US-amerikanischen *`fruit oft he poisonous tree´*-

1165 *Bizer*, Kryptokontroverse, in: *Kubicek,* Multimedia – Technik sucht Anwendung, S. 214, 220.
1166 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 210.
1167 Wie der Fall Daschner und dessen Rezeption in der öffentlichen Meinung gezeigt haben, ist eine bewusste Übertretung rechtlicher Grenzen in der Hoffnung, Leben retten zu können, ein durchaus realistisches Szenario.

Doktrin entsprechende Nichtberücksichtigung von Beweisen, die erst aufgrund eines unverwertbaren Beweises gefunden wurden, fremd ist.[1168]

Auch wenn man davon ausgehen möchte, dass sich die Sicherheitsbehörden innerhalb der Grenzen einer richterlichen Anordnung halten, ist der Tatsache Rechnung zu tragen, dass die Schlüssel kompromittiert sind und der Betroffene ohne Kenntnis von der Abhörmaßnahme keinen Anlass hat, seine Kommunikation durch neue Schlüssel wieder sicher zu gestalten:

> „Da der Betroffene nach deutschem Recht erst über die Abhörmaßnahme informiert wird, wenn ihr Zweck nicht mehr gefährdet ist, kann er die Vertraulichkeit seiner Kommunikation erst sehr viel später durch neue Schlüssel wieder herstellen."[1169]

(8) Sinkende Vertrauenswürdigkeit von Verschlüsselung

Da der Einzelne, der zugelassene *`key escrow´*- oder *`key recovery´*-Verschlüsselungsverfahren nutzt, nicht nur eine ihm nicht mitgeteilte staatliche Abhörmaßnahme, sondern auch eine Kompromittierung der Sicherungsinfrastruktur zur Verwaltung der Schlüsselduplikate bzw. der Nachschlüsselinformationen befürchten muss, sinkt die Vertrauenswürdigkeit von Verschlüsselung – mit den daraus folgenden Verunsicherungseffekten.

> „Andererseits sind seine Schutzmaßnahmen nur solange wirksam, wie die Verwaltung der Schlüssel nicht kompromittiert ist. Hierbei ist zu bedenken, daß die Vertrauenswürdigkeit der Verschlüsselungsverfahren allein schon durch die Möglichkeit staatlichen Zugriffs erheblich gefährdet wird."[1170]

(9) Datenschutzrechtliche Bedenken

Zuletzt wurden auch noch datenschutzrechtliche Bedenken gegen ein Schlüsselhinterlegungs- oder Nachschlüsselmodell vorgebracht, da dies einen Verstoß gegen das aus dem Volkszählungsurteil hergeleitete Verbot der Vorratsdatenspeicherung bedeuten könnte:

> "Das Lizenzierungsmodell ist zudem auch datenschutzrechtlich problematisch, weil es voraussetzt, daß die Anbieter von Kryptoverfahren die geheimen Verschlüsselungsschlüssel ihrer Kunden allein nur für den Fall aufbewahren, daß sie möglicherweise in der Zukunft von den Sicherheitsbehörden benötigt werden könnten, ohne daß heute nähere Verdachtsmomente die Speicherung rechtfertigen müßten. Eine flächendeckende Speicherungspflicht `zu unbestimm-

1168 Auch der EGMR hat in seiner Entscheidung im Fall Gäfgen in einer solchen Praxis zwar eine starke Vermutung für ein unfaires Verfahren (Verstoß gegen Art. 6 EMRK) aber nicht automatisch ein unfaires Verfahren gesehen; vgl. EGMR, Urteil vom 30.06.2008, Az.: 22978/05, Rn. 105. Allerdings hat die Große Kammer des EGMR einen entsprechenden Antrag auf Verweisung der Rechtssache an sie (Art. 43 EMRK) angenommen, so dass eine endgültige Entscheidung noch aussteht.

1169 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 210 f.

1170 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 210.

ten oder noch nicht bestimmbaren Zwecken´ steht aber im Widerspruch zum Verbot der `Vorratshaltung personenbezogener Daten´.“[1171]

Allerdings ist das BVerfG in seiner Entscheidung zur Vorratsdatemspeicherung merklich von dem „strikten Verbot einer Speicherung von Daten auf Vorrat“[1172] abgerückt, indem es auch eine *sechsmonatige anlasslose* Speicherung von Telekommunikationsverkehrsdaten am Verhältnismäßigkeitsgrundsatz messen und nicht dem strikten Vorratsdatenspeicherungsverbot unterfallen lassen will.[1173] Ob bei dieser Sachlage noch von einem „strikten Verbot“ gesprochen werden kann, ist zweifelhaft:

„Strikt verboten ist lediglich die Speicherung von personenbezogenen Daten auf Vorrat zu unbestimmten und noch nicht bestimmbaren Zwecken. Eine vorsorglich anlasslose Datenspeicherung ist allerdings nur ausnahmsweise zulässig. Sie unterliegt sowohl hinsichtlich ihrer Begründung als auch hinsichtlich ihrer Ausgestaltung, insbesondere auch in Bezug auf die vorgesehenen Verwendungszwecke, besonders strengen Anforderungen.“[1174]

(10) Abwägung

Im Vergleich mit einem absoluten Verschlüsselungsverbotsgesetz wäre ein relatives Verschlüsselungsverbotsgesetz zwar weniger eingriffsintensiv, da – je nachdem, welche Verschlüsselungsverfahren zugelassen wären – Schutz gegenüber der Kenntnisnahme interessierter Dritter gewährleistet würde. Ist dieses Schutzniveau gering (Schutz nur gegen zufällige Kenntnisnahme und einfache Abhörversuche) wie etwa beim Unterszenario 2a, büßt auch ein relatives Verschlüsselungsverbot aber wenig von seiner Eingriffsintensität ein. Dem stehen zusätzlich noch effektivere Umgehungsmöglichkeiten des Verschlüsselungsverbots gegenüber. Auch ein etwas höheres Sicherheitsniveau – wie für das Unterszenario 2b festgestellt – kann gerade bei den ernsthafteren Bedrohungen der IT-Sicherheit durch technisch versierte Kriminelle, Organisierte Kriminalität und ausländische Sicherheitsbehörden nichts ausrichten.

Lediglich in den Unterszenarien 2c und 2d wird ein grundsätzlich für den Nutzer sicheres Verschlüsselungsverfahren zugelassen, das die Qualität des Eingriffs in das Fernmeldegeheimnis stark absenkt: gegen Angriffe Dritter grundsätzlich gesicherte Kommunikation wird ermöglicht.[1175] Ein relatives Verschlüsselungsverbot würde

1171 *Bizer,* KritJ 1995, 450, 463 unter Zitierung des Volkszählungsurteil (BVerfGE 65, 1, 46).

1172 BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 205.

1173 BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 205.

1174 BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 206.

1175 In der US-amerikanischen Debatte um den sog. Clipper-Chip und den diesem zu Grunde liegenden `*Escrowed Encryption Standard´*(EES) wurde laut *Froomkin,* U. Pa. L. Rev. 1995, 709, 744 (allerdings für die Telefonüberwachung) dementsprechend argumentiert, ein Schlüsselhinterlegungsmodell würde eigentlich den status quo beibehalten: Kommunikation wäre wie bisher nicht gegenüber staatlicher Kenntnisnahme geschützt – mit dem `*Escrowed Encryption Standard´* aber wenigstens sicherer gegenüber der Kenntnisnahme nicht-staatlicher Dritter.

dann aber eine Infrastruktur zur Verwaltung von Schlüsselduplikaten oder Nachschlüsselinformationen benötigen, die Angriffe auf diese „höchst sicherheitsempfindlichen Stellen“[1176] möglich erscheinen lassen. Vor allem aber besteht eine Konfliktsituation zwischen Verschlüsselungsverfahren mit hinterlegtem Schlüsselduplikat oder Nachschlüssel einerseits und der Sicherheit und Vertrauenswürdigkeit der digitalen Signatur andererseits. Da beides auf derselben Technologie – der asymmetrischen Verschlüsselung – basiert, sollte sinnvollerweise für beides ein identisches Sicherheitsniveau gelten. Andernfalls wird eine der beiden Anwendungen korrumpiert werden.

Da eine gesetzliche Regelung zur digitalen Signatur – im Gegensatz zu einer Reglementierung von Verschlüsselungsverfahren – bereits existiert, ist die Abwägungsentscheidung zunächst auf dieser Tatsachenbasis zu treffen. Der Zielkonflikt zwischen den Sicherheitsanforderungen der digitalen Signatur einerseits und den Unsicherheitsanforderungen für ein Verschlüsselungsverfahren mit Nachschlüssel oder hinterlegtem Schlüsselduplikat andererseits, müsste im Rahmen der Verhältnismäßigkeit im engeren Sinne Berücksichtigung finden. Gleiches gilt für die durch die digitale Signatur und die zugelassenen Verschlüsselungsverfahren erleichterten Umgehungsmöglichkeiten des relativen Verschlüsselungsverbots. Die geringere Eingriffsqualität kann diese Nachteile nicht ausgleichen. Daher wäre auch ein relatives Verschlüsselungsverbot mit Nachschlüssel oder Schlüsselhinterlegung unverhältnismäßig.

Denkbar wäre grundsätzlich auch, dass mit der Einführung eines relativen Verschlüsselungsverbots die digitale Signatur abgeschafft würde. Allerdings scheinen die politischen Tendenzen eher in Richtung einer Stärkung von E-Government[1177], und damit von Vertraulichkeit *und* rechtlicher Verbindlichkeit, zu gehen.[1178] Letztlich wäre ein relatives Verschlüsselungsverbot auch dann unverhältnismäßig, da die Vertraulichkeit der Kommunikation eingeschränkt wird, ohne dass daraus tatsächlich ein Sicherheitsgewinn entsteht, da jeder das Verbot auf einfachste Weise umgehen kann.

4. Ergebnis

Ein relatives Verschlüsselungsverbotsgesetz würde daher – gleichgültig in welcher konkreten Ausgestaltung – einen Verstoß gegen das Fernmeldegeheimnis (Art. 10 I GG) darstellen.

1176 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 210.

1177 Unter E-Government versteht man nach der sog. Speyerer Definition "die Abwicklung geschäftlicher Prozesse in Zusammenhang mit Regieren und Verwalten (Government) mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien.“; zitiert nach *Paul,* JurPC 144/2008, Rn. 186.

1178 Vgl. etwa das Programm „E-Government 2.0“ der Bundesregierung; verfügbar unter: http://www.kbst.bund.de/cln_028/nn_836958/Content/Egov/Initiativen/EGov2/EGov2.html__nnn=true (19.09.2008).

II. Verstoß gegen das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 I GG)

Ein relatives Verschlüsselungsverbotsgesetz würde auch einen Verstoß gegen das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 I GG) darstellen (s.o. in Teil 3 unter A.II.). Das Grundrecht gewährleistet auch den Einsatz von Verschlüsselung. Ein Verbot von Verschlüsselungsverfahren unter Gestattung der Nutzung bestimmter staatlich lizenzierter Verfahren, die Zugriffsmöglichkeiten staatlicher Sicherheitsbehörden sicherstellen, würde einen Eingriff in dieses Recht darstellen. Dieser Eingriff wäre mangels einer entsprechenden Schrankenregelung in Art. 13 GG verfassungsrechtlich nicht zu rechtfertigen.

III. Verstoß gegen das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG)

Ein relatives Verschlüsselungsverbotsgesetz würde wie ein absolutes Verschlüsselungsverbot auch einen Eingriff in das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG), insbesondere in seinen Ausprägungen als Recht auf informationelle Selbstbestimmung und als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, darstellen (s.o. in Teil 3 unter A.III.). Ein verdachtsunabhängiges Verbot gegenüber jedermann, seine Daten effektiv gegen Kenntnisnahme zu schützen, würde im Hinblick auf die Betroffenheit von Daten, die zum absolut geschützten Kernbereich privater Lebensgestaltung gehören, gegen die Wesensgehaltsgarantie (Art. 19 II GG) verstoßen (s.o. in Teil 3 unter A. III.3.b.). Ein relatives Verschlüsselungsverbot wäre des Weiteren mit parallelen Argumenten, wie sie eben für das Fernmeldegeheimnis dargestellt wurden (s.o. unter I.3.c.dd)), unverhältnismäßig. Zusätzlich ist im Rahmen der Abwägungsentscheidung zu berücksichtigen, dass ein besonders schwerer Eingriff in das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) vorliegt, da das allgemeine Persönlichkeitsrecht eine Schutzbereichsverstärkung durch Art. 4 I GG, Art. 6 I GG, Art. 5 I S. 1 GG, Art. 8 I GG und Art. 9 I, III GG als partiell spezielle Privatsphärengewährleistungen erfährt (s.o. in Teil 3 unter A.III.1.f.cc)(2)(b)). Ein relatives Verschlüsselungsverbotsgesetz wäre daher nicht verhältnismäßig im engeren Sinne.

B. Verschlüsselungsverbot und wirtschaftliche Betätigungsfreiheit

I. Verstoß gegen die Eigentumsfreiheit (Art. 14 I S. 1 GG)

Ein relatives Verschlüsselungsverbotsgesetz würde gleichfalls einen Eingriff in die Eigentumsfreiheit (Art. 14 I S. 1 GG) darstellen. Die Möglichkeiten zum Schutz von Betriebs- und Geschäftsgeheimnissen durch Verschlüsselungsverfahren würden beschränkt. Auch die innerhalb des Szenarios eines relativen Verschlüsselungsverbots sichersten Varianten – ein Schlüsselhinterlegungs- oder ein Nachschlüsselmodell –

können angesichts der Angreifbarkeit der Sicherungsinfrastruktur gerade *keinen* effektiven Schutz gegen die potentesten Angreifer bieten – die ausländischen Sicherheitsbehörden. Angesichts der höchst zweifelhaften Geeignetheit eines Verschlüsselungsverbots kann dieser Eingriff nicht als verhältnismäßig angesehen werden.

II. Verstoß gegen die Berufsfreiheit (Art. 12 I GG)

Ein relatives Verschlüsselungsverbotsgesetz würde ebenfalls in die Berufsfreiheit (Art. 12 I GG) eingreifen:

- Soweit es um die *Entwicklung, Herstellung und schließlich den Vertrieb von Verschlüsselungsprodukten* geht, wäre der Eingriff im Rahmen eines relativen Verschlüsselungsverbots wesentlich weniger intensiv, da alle Tätigkeiten weiterhin möglich sind. Dabei sind nur bestimmte staatliche Anforderungen an die Ausgestaltung von Verschlüsselungsverfahren einzuhalten. Es handelt sich somit um einen Eingriff in die Berufsausübungsfreiheit.[1179] Die nach staatlichen Vorgaben ausgestalteten Verschlüsselungsprodukte mögen nicht in gleichem Maße das Kundeninteresse wecken, wie dies bei auch gegenüber staatlichen Abhörmaßnahmen sicheren Verschlüsselungsverfahren der Fall wäre. Gewinnchancen werden aber regelmäßig[1180] nicht durch die Berufsfreiheit geschützt.
- Ein relatives Verschlüsselungsverbotsgesetz würde daneben einen Eingriff in die von Art. 12 I GG geschützten *Berufsgeheimnisse* darstellen. Auch hierbei liegt ein Eingriff in die Berufsausübungsfreiheit vor. Allerdings sind auch bei einem relativen Verschlüsselungsverbot die Grundbedingungen der Berufsausübung betroffen. Die Vertraulichkeitsgebote sollen gerade auch gegen staatliche Kenntnisnahme schützen. Dieser Schutz wird durch ein relatives Verschlüsselungsverbot vereitelt.

Das Verbot der Entwicklung, Herstellung und des Vertriebs von Verschlüsselungsverfahren kann im Hinblick auf die gewichtigen Allgemeinwohlbelange, denen ein relatives Verschlüsselungsverbot zu dienen bestimmt ist, verfassungsrechtlich gerechtfertigt werden. Anders ist dies bezüglich der Berufsgeheimnisse zu bewerten: Der Eingriff betrifft die Grundbedingungen der Berufsausübung. Auch die gewichtigen Belange der Straftatverfolgung und –prävention können diesen Eingriff nicht rechtfertigen.

1179 So auch *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 209.

1180 Dies kann anders sein, wenn Absatzschwierigkeiten oder Umsatzrückgänge erdrosselnde Wirkung haben.

III. Verstoß gegen besondere Berufs- und Geschäftsgeheimnisse

Soweit bereichsspezifische Berufsgeheimnisse (Pressefreiheit nach Art. 5 I S. 2 GG, Religionsfreiheit nach Art. 4 I GG sowie die Freiheit des Mandats aus Art. 38 I S. 2 GG) oder Betriebs- und Geschäftsgeheimnisse (Wissenschaftsfreiheit nach Art. 5 III S. 1 GG) existieren, würde ein relatives Verschlüsselungsverbotsgesetz auch in diese eingreifen. Auch dieser spezielle grundrechtliche Geheimnisschutz will den Schutz vor staatlicher Kenntnisnahme bewirken. Die alleinige Zulassung von Verschlüsselungsverfahren, die gegenüber staatlicher Kenntnisnahme keinen Schutz gewährleisten, würde daher einen Eingriff darstellen. Angesichts der hohen Bedeutung der grundrechtlichen Vertraulichkeitsgewährleistungen – sowohl für den Einzelnen als auch für ein demokratisches Gemeinwesen – ist ein Eingriff auch zu Gunsten gewichtiger Allgemeinrechtsgüter nicht verfassungsrechtlich zu rechtfertigen.

C. Verschlüsselungsverbot und Gleichheitsverstoß

Zuletzt würde auch ein relatives Verschlüsselungsverbotsgesetz einen Verstoß gegen das Willkürverbot (Art. 3 I GG) darstellen. Aufgrund der tatsächlichen Rechtsdurchsetzungsdefizite wird nur derjenige von einem Verschlüsselungsverbot betroffen, der aus Unkenntnis, Gesetzestreue und/oder fehlender Sensibilität hinsichtlich des Schutzes personenbezogener Information freiwillig dem Verbot Folge leistet.

> „Auch ein staatliches Linzensierungsmodell von Kryptoverfahren wird die Verwendung nicht lizensierter Verschlüsselungsverfahren nicht unterbinden können. Straftäter, Verfassungsfeinde und andere Objekte staatlicher Überwachung werden ihre Kommunikation auch trotz Verbot mit nicht zugelassenen Kryptoverfahren sichern können.“[1181]

Eine Umgehung des Verschlüsselungsverbots ist schwierig feststellbar, verdachtsunabhängige Kontrollbefugnisse zur Überprüfung der Einhaltung eines Verschlüsselungsverbots würden einen verfassungsrechtlich nicht zu rechtfertigenden Eingriff in das Fernmeldegeheimnis darstellen. Verschlüsselte Daten können nicht nur im Wege der Steganographie sondern auch durch schlichtes Überschlüsseln mit einem zugelassenen Verschlüsselungsverfahren getarnt werden. Neben der Schwierigkeit, das Vorliegen einer Verschlüsselung zu beweisen, ist auch eine wirksame Sanktionierung in verhältnismäßiger Weise kaum oder überhaupt nicht möglich.

Der Ehrliche[1182] wäre also durch symbolisches Recht betroffen, das gegenüber denjenigen, die dieses Recht treffen soll, wirkungslos bleiben muss:

> „Letztlich würde das Lizensierungsmodell nur dazu führen, daß das Fernmeldegeheimnis normaler Teilnehmer staatlichem Zugriff technisch ungeschützt preisgegeben wäre, hingegen

1181 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 211.

1182 Oder - mit *Bryde*, Die Effektivität von Recht als Rechtsproblem, S. 20 - der Dumme, der Pechvogel etc.

würde sich die Klientel der Behörden der inneren Sicherheit gegen deren Abhörversuche durch nicht zugelassene Kryptoverfahren erfolgreich schützen können.“[1183]

1183 *Bizer*, Die Kryptokontroverse, in: *Hammer,* Sicherungsinfrastrukturen, S. 179, 211.

Teil 5: Grundrecht auf Verschlüsselung im Kontext von Pflichten zur Schlüsselherausgabe

Als „goldener Mittelweg“ könnte sich die Etablierung von gesetzlichen Verpflichtungen zur Herausgabe von verwendeten Schlüsseln oder Passwörtern erweisen, was in Deutschland immer wieder von Seiten der Sicherheitsbehörden gefordert wird[1184] und international in vielen Staaten Rechtslage ist.[1185] Diese Lösung des Konflikts von Freiheits- und Sicherheitsinteressen erscheint simpel und praktikabel: Der Einzelne könnte seine Kommunikation und seine Daten gegenüber Dritten und grundsätzlich auch gegenüber dem Staat durch Verschlüsselungsverfahren geheim halten. Besteht jedoch der hinreichende Tatverdacht der Begehung einer Straftat[1186] könnten die Strafverfolgungsbehörden auf die verschlüsselten Daten zugreifen. In einem solchen

Szenario 3
Staat S verpflichtet per Gesetz zur Herausgabe von verwendeten Schlüsseln und Passwörtern.

kann jeweils nach der Person des Verpflichteten unterschieden werden:

- Herausgabepflichtig könnten zum einen die Betroffenen, d.h. die *Beschuldigten* selbst sein.
- Herausgabepflichtig könnten aber auch private *Dritte* (als Zeugen) sein, die aus irgendwelchen Gründen Schlüssel oder Passwörter kennen.[1187]
- Schließlich könnten auch *Diensteanbieter*, die die Verwendung von Verschlüsselungsoptionen anbieten, verpflichtet werden, Schlüssel oder Passwörter herauszugeben.[1188]

1184 Vgl. heise online vom 24.10.2007, Bitkom will Onlinedurchsuchung mit Sachverstand diskutieren, verfügbar unter: http://www.heise.de/newsticker/meldung/97911 (16.11.2007).

1185 S.o. in Teil 2 unter B.III.

1186 Und ggf. weitere Erfordernisse wie die „wesentliche Erschwernis oder Aussichtslosigkeit der Erforschung des Sachverhalts auf andere Weise“; vgl. insoweit die Voraussetzungen für eine Telekommunikationsüberwachung (§ 100a I Nr. 3 StPO), Abhörmaßnahmen in einer Wohnung (sog. Lauschangriff, § 100c I Nr. 3 StPO) oder Abhörmaßnahmen außerhalb von Wohnungen (§ 100f I letzter Hs. StPO).

1187 Dabei ist – vor allem für vom Beschuldigten selbst gespeicherte Daten – insbesondere an die Systemadministratoren zu denken. Daneben fallen all jene Konstellationen hierunter, in denen Daten bei Dritten gespeichert sind, etwa Kontoinformationen bei Banken (vgl. dazu *Radtke*, Aktive Mitwirkungspflichten und die "freiwillige" aktive Mitwirkung des Betroffenen bei dem Zugriff auf elektronisch gespeicherte Daten im Strafprozess, in: *Eser/Goydke/Maatz/ Meurer,* Strafverfahrensrecht in Theorie und Praxis, S. 321).

1188 Es würde den Rahmen dieser Arbeit sprengen, alle insoweit denkbaren Optionen durchzuspielen. Hier ist zunächst der einfachste Fall gemeint, dass der Diensteanbieter Kopien der Schlüssel und Passwörter ohnehin im Rahmen seines Geschäftsmodells gespeichert vorhält.

A. Herausgabepflicht von Beschuldigten

Beschuldigte sind grundsätzlich nicht verpflichtet, sich zu der Beschuldigung zu äußern, und sind auch dementsprechend zu belehren (§ 136 I S. 2 StPO).[1189] Diese Aussagefreiheit ist Ausdruck des Grundsatzes, dass niemand verpflichtet ist, sich selbst zu belasten (nemo-tenetur-Prinzip: *`nemo tenetur se ipsum accusare´*) und als solche Kernstück des Rechts auf ein faires Verfahren[1190] und übergeordneter verfassungsrechtlicher Grundsatz (etwa verankert in Art. 14 III lit. g IPbpR).[1191] Umstritten ist aber zum einen, wie weit das Verbot des Selbstbelastungszwangs reicht (I.), und zum anderen, inwieweit dieses Aussageverweigerungsrecht eingeschränkt werden könnte (II.).

I. Reichweite des Schutzes vor Selbstbelastung

Der Schutz vor Selbstbelastung bewahrt den Beschuldigten davor, *aktiv* zu seiner Strafverfolgung beitragen zu müssen.[1192] Dementsprechend wird zwischen aktiver Mitwirkung, die der Beschuldigte gerade nicht leisten muss, einerseits und passiver Duldung von Ermittlungsmaßnahmen andererseits unterschieden. Letztere unterfallen nicht dem Verbot des Selbstbelastungszwanges, und der Beschuldigte muss sie hinnehmen. Dazu gehören etwa die Untersuchung des psychischen (§ 81 StPO) oder körperlichen (§ 81a StPO) Zustands des Beschuldigten oder die Duldung von Gegenüberstellungen (§ 58 II StPO). So auch die Rechtsprechung des BVerfG:

> „Am weitesten reicht der Schutz gegen Selbstbezichtigungen für Zeugen, Prozeßparteien und insbesondere für Beschuldigte im Strafverfahren und in anderen Verfahren. Soweit für diesen Personenkreis ein Zwang zur Mitwirkung besteht, der zu strafrechtlichen Nachteilen führen kann (Entnahme von Blutproben und Untersuchungen zur Feststellung der Abstammung gemäß §§ 81a ff. StPO, § 327a ZPO, Wartepflicht am Unfallort gemäß § 142 StGB), handelt es sich um passive, im Schrifttum teilweise als bedenklich beanstandete Duldungs- und Verhaltenspflichten, die im vorliegenden Zusammenhang außer acht bleiben können.“[1193]

Diese Grenzziehung von aktiver Mitwirkung zu passiver Duldung ist in der Sache überzeugend: Das Verbot des Selbstbelastungszwanges dient dazu, den Beschuldigten vor der Konfliktsituation zu bewahren, sich zwischen drei jeweils für ihn nach-

> Dies kann er ohne Weiteres in seinen Geschäftsbedingungen so vorsehen. Zumal es auch im Sinne der Kunden sein kann, da Daten bei einem Verlust des Schlüssels oder Vergessen des Passworts nicht unwiederbringlich verloren sind (weil durch angriffsresistente Verschlüsselung geschützt). Eine gesetzliche Verpflichtung der Diensteanbieter, Schlüssel und Passwörter zu speichern, dürfte dagegen auf die im Rahmen der relativen Verschlüsselungsverbote erörterten Sicherheitsbedenken stoßen.

1189 Siehe *Meyer-Goßner,* StPO, § 136, Rn. 7.
1190 BVerfGE 38, 105, 113.
1191 *Bär*, Handbuch zur EDV-Beweissicherung, S. 440.
1192 *Diemer*, in: *Hannich,* KK StPO, § 136, Rn. 10.
1193 BVerfGE 56, 37, 42.

teiligen Folgen entscheiden zu müssen, nämlich sich entweder selbst zu belasten oder eine Falschaussage zu begehen oder von der Anwendung von Zwangsmitteln bedroht zu sein.[1194] Diese Konfliktsituation entsteht in der beschriebenen Weise aber nur, soweit es um aktive Mitwirkungshandlungen geht.

So klar die Unterscheidung von aktiver Mitwirkung und passiver Duldung in der Theorie erscheint, so umstritten kann in der Praxis im Einzelfall die Kategorisierung sein. Der zwangsweise Einsatz von Brechmitteln (der in der Regel erfolgt, um als Drogendealer oder –kuriere verdächtigte Personen dazu zu bringen, die in Päckchen im Magen transportierte Ware zu erbrechen) wurde etwa teilweise als zulässig – da passive Duldung[1195] – und teilweise als unzulässig – da aktive Mitwirkung[1196] – angesehen. Ausgehend von diesem Kritikpunkt der mangelnden Trennschärfe des Unterscheidungskriteriums Aktivität-Passivität wurde die Anwendung des nemo-

1194 Dagegen sieht *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 1, Rn. 56 das Aussageverweigerungsrecht von Beschuldigten dadurch begründet, dass angesichts des Folterverbots eine Möglichkeit zur Erzwingung von Aussagen fehle. Dies könnte man aber ebenso von jeder Zeugenaussage behaupten; eine Aussageerzwingung kann immer nur mittelbar über die Androhung und Verhängung von Ordnungs- oder Zwangsmitteln erfolgen, da eine Aussage eine unvertretbare Handlung darstellt. Die unterschiedliche Behandlung von Zeugen- und Beschuldigtenaussage vermag *Starck* mit seinem Ansatz nicht zu begründen.

1195 So etwa BVerfG, Beschluss vom 15.09.1999, Az.: 2 BvR 2360/95, Rn. 4; *Hillgruber*, in: *Epping/Hillgruber,* Beck-OK GG, Art. 1, Rn. 41. Weitere Nachweise zum Streitstand bei *Kutscha*, Innere Sicherheit und Freiheitsrechte, in: *Roggan/Kutscha,* Handbuch zum Recht der Inneren Sicherheit, S. 28, 34.

1196 Vgl. OLG Frankfurt a. M., Urteil vom 11.10.1996, Az.: 1 Ss 28/96, NJW 1997, 1647, 1648: "Die zwangsweise Verabreichung eines Brechmittels verstößt gegen diesen Grundsatz der Passivität. Denn sie soll den Beschuldigten zwingen, aktiv etwas zu tun, wozu er nicht bereit ist, nämlich sich zu erbrechen. Das ist weder im Rahmen des § 81a StPO erlaubt noch mit der allgemeinen Stellung des Beschuldigten im Strafverfahren zu vereinbaren." Auch der EGMR hat den Einsatz von Brechmitteln als Verstoß gegen das in Art. 6 I EMRK als Teil des Rechts auf ein faires Verfahren verbürgte Recht, sich nicht selbst zu beschuldigen, angesehen: „Having regard to the foregoing, the Court would also have been prepared to find that allowing the use at the applicant's trial of evidence obtained by the forcible administration of emetics infringed his right not to incriminate himself and therefore rendered his trial as a whole unfair." (EGMR, Urteil der großen Kammer vom 11.07.2006, Az.: 54810/00, Jalloh/Deutschland, Rn. 122). Allerdings hält der EGMR die Verwertung von „Beweismaterial, das vom Angeklagten durch Zwang gewonnen werden kann, aber unabhängig vom Willen des Betroffenen vorhanden ist" (`material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect´, vgl. ebenda, Rn. 112; Übersetzung nach NJW 2006, 3117, 3124) grundsätzlich nicht für unzulässig. Zum Teil hat der EGMR aber Fälle von Zwangsanwendung zur Gewinnung körperlicher Beweise in das Recht, sich nicht selbst zu beschuldigen, einbezogen und sodann im Rahmen einer Gesamtabwägung entschieden, ob eine Verletzung von Art. 6 I EMRK vorliegt: „However, the Court has on occasion given the principle of self-incrimination as protected under Article 6 § 1 a broader meaning so as to encompass cases in which coercion to hand over real evidence to the authorities was at issue." (ebenda, Rn. 111).

tenetur-Grundsatzes von einigen Stimmen in der Literatur auf die reine *Aussage*freiheit im Strafverfahren reduziert.[1197]

Allerdings herrscht auch hinsichtlich der Abgrenzung einer Aussage in diesem Sinne und einer Herausgabe Unklarheit: Handelt es sich bei der Nennung von Passwörtern um eine Aussage oder um eine Herausgabe von Daten? Die Parallele zu einer Aussage liegt nahe, da es in der Regel um die mündliche Nennung von Passwörtern, die ansonsten nirgendwo fixiert sind, geht. Für die Annahme einer Herausgabe spricht dagegen, dass die Nennung von Schlüsseln oder Passwörtern regelmäßig anlässlich von Durchsuchungen nach §§ 102, 103 StPO relevant wird.[1198] Die Herausgabe von Gegenständen bestimmt sich dabei nach § 95 I StPO. Auch wenn sich die strafprozessuale Editionspflicht aus § 95 I StPO nach dem Wortlaut nur auf „Gegenstände" bezieht, wird die Vorschrift allgemein auch auf die Herausgabe von Daten, mithin auch Schlüsseln oder Passwörtern, angewendet. Dafür spricht die systematische Stellung von § 95 StPO: Die darin normierte Herausgabepflicht des Gewahrsamsinhabers bezieht sich auf § 94 StPO, der Sicherstellung und Beschlagnahme von (potentiellen) Beweismitteln regelt. Datenträger und digital gespeicherte Informationen können Gegenstand von Sicherstellung und Beschlagnahme nach § 94 StPO sein.[1199] Daher ist auch die Editionspflicht des § 95 StPO auf Daten und Datenträger anwendbar. Eine Reduktion des nemo-tenetur-Grundsatzes auf die Freiheit des Beschuldigten, sich nicht selbst *durch seine Aussage* belasten zu müssen, führt also nicht zu größerer Klarheit in der Konturierung der Reichweite des Grundsatzes im Einzelfall.

Es bleibt daher bei der im Wege teleologischer Auslegung ermittelten Grenze des nemo-tenetur-Grundsatzes, wonach der Beschuldigte keine aktive Mitwirkung leisten muss, aber zur passiven Duldung von Ermittlungsmaßnahmen verpflichtet ist.[1200] Die Nennung oder Herausgabe von Passwörtern oder Schlüsseln würde eine aktive Mitwirkungshandlung des Beschuldigten bedeuten, er müsste aktiv sein Passwort oder den verwendeten Schlüssel nennen. Nach dem nemo-tenetur-Grundsatz darf der Beschuldigte dazu nicht verpflichtet werden.[1201] Beschuldigte sind nicht verpflichtet,

1197 *Radtke*, Aktive Mitwirkungspflichten und die "freiwillige" aktive Mitwirkung des Betroffenen bei dem Zugriff auf elektronisch gespeicherte Daten im Strafprozess, in: *Eser/Goydke/Maatz/Meurer,* Strafverfahrensrecht in Theorie und Praxis, S. 321, 330 f. m.w.N.

1198 EDV-Anlagen sind zulässige Durchsuchungsgegenstände; *Meyer-Goßner,* StPO, § 102, Rn. 10 f. Herausgabeverlangen kommen naturgemäß nur bei offenen Ermittlungsmaßnahmen in Betracht und nicht bei heimlichen wie bei der Überwachung der Telekommunikation. Vgl. allg. zu Durchsuchungen von EDV-Anlagen *Bär,* CR 1995, 158-169, 227-234.

1199 *Meyer-Goßner,* StPO, § 94, Rn. 4.

1200 *Meyer-Goßner,* StPO, § 95, Rn. 5.

1201 Dafür spricht auch § 95 II S. 2 StPO, der die Festsetzung von Ordnungs- oder Zwangsmitteln bei nicht erfolgter Herausgabe von Gegenständen gegen Zeugnisverweigerungsberechtigte untersagt.

Passwörter oder verwendete Schlüssel herauszugeben.[1202] Dem entspricht auch die Praxis der Ermittlungsbehörden.[1203]

II. Einschränkbarkeit des Aussageverweigerungsrechts?

De lege lata kann die Preisgabe von Schlüsseln oder Passwörtern vom Beschuldigten nicht verlangt werden. Zu prüfen bleibt, ob eine gesetzliche Herausgabepflicht geschaffen und das Aussageverweigerungsrecht von Beschuldigten entsprechend eingeschränkt werden könnte. Dabei ist umstritten, ob eine solche gesetzliche Herausgabeverpflichtung an der Menschenwürde (Art. 1 I GG) oder lediglich am allgemeinen Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) oder am Auffanggrundrecht der allgemeinen Handlungsfreiheit (Art. 2 I GG) zu messen ist.[1204]

Nach einer in der Literatur vertretenen Auffassung kann es niemals die Menschenwürde eines Beschuldigten verletzen, wenn dieser gezwungen wird, die Konsequenzen seiner Handlungen zu tragen (im Fall seiner Schuld) oder sich zu entlasten (im Fall seiner Unschuld).[1205] Es berührt dieser Auffassung zufolge nicht die Menschenwürde, wenn der Staat aus dem Schweigen des Angeklagten Schlüsse zieht. Der Angeklagte sei nicht bloßes Objekt staatlichen Handelns, sondern könne sich vielmehr durch seine Möglichkeiten, sich zu äußern, als Subjekt in die Wahrheitsfindung einschalten.

Andere Stimmen in der Literatur sowie das BVerfG sehen den nemo-tenetur-Grundsatz dagegen in der Menschenwürde verankert:[1206]

> „Ein Zwang zur Selbstbezichtigung berührt zugleich die Würde des Menschen, dessen Aussage als Mittel gegen ihn selbst verwendet wird.“[1207]

Demnach wäre das Aussageverweigerungsrecht nicht einschränkbar. Das BVerfG betont aber, dass es

> „kein ausnahmsloses Gebot [gebe; d. Verf.], daß niemand zu Auskünften oder zu sonstigen Handlungen gezwungen werden darf, durch die er eine von ihm begangene strafbare Handlung offenbart.“[1208]

1202 So auch *Bär*, Handbuch zur EDV-Beweissicherung, S. 399 sowie *Bizer,* KritJ 1995, 450, 462.

1203 Vgl. die Beispiele Vetter, law blog, 2 x nein, verfügbar unter: http://www.lawblog.de/index.php/archives/2009/01/06/2-x-nein/ (06.01.2009) sowie Vetter, law blog, Verschlüsseln macht verdächtig, verfügbar unter: http://www.lawblog.de/index.php/archives/2009/02/24/verschluesseln-macht-verdachtig/ (24.03.2009).

1204 Für eine Betroffenheit der Menschenwürde *Dreier*, in: *Dreier,* GG, Art. 1, Rn. 140 m.w.N.; gegen eine Betroffenheit der Menschenwürde *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 1, Rn. 56.

1205 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 1, Rn. 56.

1206 *Dreier*, in: *Dreier,* GG, Art. 1, Rn. 140 mit vielen weiteren Nachweisen; BVerfGE 55, 144, 150; 56, 37, 42.

1207 BVerfGE 56, 37, 42.

1208 BVerfGE 56, 37, 42.

Das BVerfG differenziert insoweit nach der Rolle der Auskunftsperson und der Zweckbestimmung der Auskunft:[1209]

- Ausgehend vom strafprozessualen nemo-tenetur-Grundsatz, dessen umfassendes Schweige- und Aussageverweigerungsrecht unangetastet bleibt, sieht das BVerfG auch in anderen Verfahren, in denen die Aussage speziell *strafrechtlichen oder ähnlichen Zwecken* dient, ein *Schweigerecht* gegeben.[1210] Dieses Schweigerecht gilt auch bereits im Vorstadium vor der Einleitung förmlicher Verfahren.[1211]
- Im *Zivilprozess* besteht dagegen grundsätzlich eine *Wahrheitspflicht* (für die Parteien nach § 138 I ZPO, für Zeugen nach § 395 I ZPO). Auch hier gilt aber – neben anderen – die Ausnahme, dass der Aussagende sich nicht der Gefahr der Strafverfolgung aussetzen muss (so etwa § 384 Nr. 2 ZPO für Zeugen).
- Ausnahmen vom Grundsatz des Schweige- und Aussageverweigerungsrechts für den Fall der Selbstbezichtigung hält das BVerfG allein jenseits von Straf- oder strafähnlichen Verfahren und hinsichtlich Personen, die aus besonderen Gründen rechtsgeschäftlich oder gesetzlich zur Auskunftserteilung verpflichtet sind, für möglich.[1212] Im Übrigen kann der rechtstaatliche Grundsatz[1213] von Schweige- und Aussageverweigerungsrechten nicht eingeschränkt werden.

Die Einführung einer gesetzlichen Herausgabepflicht für verwendete Schlüssel und Passwörter wäre nach diesen Grundsätzen nicht möglich. Bedarf für eine solche Herausgabepflicht besteht klassischerweise in Konstellationen, in denen eine Einschränkung des Schweigerechts bei Zugrundelegung der bundesverfassungsgerichtlichen Maßstäbe ausscheidet:

- Eine Herausgabepflicht von Schlüsseln oder Passwörtern kommt nur in Betracht, wenn staatliche Behörden verschlüsselte Daten oder Datenträger auffinden.
- Erhält der Staat verschlüsselte Daten im Rahmen einer heimlichen Überwachungsmaßnahme, z.B. einer Telekommunikationsüberwachung, will er diese Maßnahme typischerweise nicht gegenüber den Betroffenen offenbaren – was zwangsläufige Folge einer Forderung nach Herausgabe verwendeter Schlüssel bzw. Passwörter wäre. Heimliche, auf Dauer angelegte Überwachungsmaßnahmen und Herausgabeverlangen schließen sich typischerweise aus.
- Das Bedürfnis nach einer Herausgabepflicht bzgl. Schlüsseln und Passwörtern besteht also typischerweise, wenn verschlüsselte Daten oder Datenträger im

1209 BVerfGE 37, 42.

1210 BVerfGE 56, 37, 43: „Ein solches Schweigerecht besteht entsprechend in anderen Verfahren, in denen dem Betroffenen ähnliche Sanktionen wegen seines Verhaltens drohen, etwa im Disziplinarverfahren sowie in berufsgerichtlichen Verfahren."

1211 BVerfGE 56, 37, 44.

1212 BVerfGE 56, 37, 45. Zu den Einzelheiten siehe ebenda. In der Verfassungsbeschwerde ging es um die Verfassungsmäßigkeit von Vorschriften in der Konkursordnung, die eine uneingeschränkte Aussageverpflichtung des Gemeinschuldners normieren. Nach den soeben genannten Grundsätzen hielt das BVerfG diese Aussagepflicht für verfassungsgemäß.

1213 So BVerfGE 38, 105, 113.

Rahmen von offenen Maßnahmen aufgefunden werden. Dies geschieht typischerweise bei Durchsuchungen nach §§ 102, 103 StPO[1214], mithin bei staatlichen Eingriffen in das Grundrecht auf Unverletzlichkeit der Wohnung.

- Nur Straf- oder strafähnliche Verfahren sind hinreichend gewichtig, um solche Grundrechtseingriffe zu rechtfertigen.

Die Situation der Auffindung verschlüsselter Daten liegt folglich typischerweise in Straf- oder strafähnlichen Verfahren vor – für die das BVerfG strikt am Aussageverweigerungsrecht aus dem nemo-tenetur-Grundsatz festhält.[1215] Das Aussageverweigerungsrecht von Beschuldigten hinsichtlich verwendeter Schlüssel sowie Passwörtern kann daher nicht im Wege einer gesetzlichen Herausgabeverpflichtung eingeschränkt werden.[1216]

Dem entsprechend sind in Deutschland auch Regelungen, wie sie etwa Art. 132-79 Code pénal[1217] in Frankreich[1218] trifft, nicht realisierbar: [1219]

1214 Sonstige Betretens-, Besichtigungs- und Kontrollrechten sind dagegen eher auf die Feststellung tatsächlicher Verhältnisse gerichtet (etwa die Einhaltung gesetzlicher Arbeitszeitbestimmung, Grenzwerte etc.).

1215 Im Übrigen bestünden auch Zweifel an der Verhältnismäßigkeit einer gesetzlichen Herausgabeverpflichtung, insbesondere an deren Geeignetheit: Der Verpflichtete könnte stets behaupten, er habe das Passwort vergessen. Anhaltspunkte, am Wahrheitsgehalt dieser Aussage zu zweifeln, dürften schwer zu finden sein – der Straftatverdacht allein kann dafür jedenfalls nicht ausreichen. Des Weiteren können verschlüsselte Daten auf dem eigenen Rechner so effektiv versteckt werden, dass nicht einmal die Existenz weiterer verschlüsselter Daten feststellbar ist (sog. *`plausible deniability´*, eine Eigenschaft mit der Verschlüsselungsprodukte gezielt beworben werden). Vgl. heise online vom 08.10.2007, Großbritannien: Passwort oder fünf Jahre Gefängnis, verfügbar unter: http:// www.heise.de/newsticker/meldung/97050/ (21. 11.2007); heise Security vom 18.05.2006, Britisches Innenministerium will die Herausgabe von Krypto-Schlüsseln erzwingen, verfügbar unter: http://www.heise.de/security/Britisches-Innenministerium-will-die-Herausgabe-von-Krypto-Schluesseln-erzwingen--/news/meldung/73301 (29.07. 2009).

1216 Zur Unmöglichkeit, bereits die Verwendung von Verschlüsselungsverfahren wirksam strafrechtlich zu sanktionieren siehe oben in Teil 3 unter A.I.3.c.bb)(5).

1217 Hier zitiert nach der konsolidierten Fassung vom 10.01.2009, verfügbar unter: http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719&dateTexte=20090325 (25.03.2009).

1218 Eingefügt durch Art 37 des Gesetzes Nr. 2004-575 vom 21.06.2004, verfügbar unter: http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=B484649EFB8F84B467480207EF77A9C1.tpdjo09v_1?cidTexte=JORFTEXT000000801164&dateTexte=20040622 (25.03.2009). Weiteres Beispiel ist Teil III des Britischen Regulation of Investigatory Powers Act (RIPA) aus dem Jahr 2000, der laut Kirk, Contested UK encryption disclosure law takes effect, verfügbar unter: http://www.washingtonpost.com/wp-dyn/content/article/2007/10/01/AR2007100100511.html (26.03.2009) am 01.10.2007 in Kraft getreten ist. Kommt der Beschuldigte einer solchen Offenbarungspflicht (*`disclosure requirement´*) nicht nach, drohen ihm nach Section 53 (5) bis zu zwei Jahre Haft oder eine Geldstrafe. Der Volltext von Part III RIPA 2000 ist verfügbar unter: http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_8#pt3 (26.03.2009). Weitere Beispiele s.o. in Teil 2 unter B.III.

1219 Vgl. die deutsche Übersetzung bei *Baum/Trafkowski,* CR 2002, 69, 70: „Soweit ein Mittel der Kryptologie i.S.d. Art. 36 des Gesetzes über die Informationsgesellschaft verwendet wurde,

“Article 132-79 Code pénal

Lorsqu'un moyen de cryptologie au sens de l'article 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission, le maximum de la peine privative de liberté encourue est relevé ainsi qu'il suit :

1° Il est porté à la réclusion criminelle à perpétuité lorsque l'infraction est punie de trente ans de réclusion criminelle;

2° Il est porté à trente ans de réclusion criminelle lorsque l'infraction est punie de vingt ans de réclusion criminelle;

3° Il est porté à vingt ans de réclusion criminelle lorsque l'infraction est punie de quinze ans de réclusion criminelle;

4° Il est porté à quinze ans de réclusion criminelle lorsque l'infraction est punie de dix ans d’emprisonnement;

5° Il est porté à dix ans d'emprisonnement lorsque l'infraction est punie de sept ans d’emprisonnement;

6° Il est porté à sept ans d'emprisonnement lorsque l'infraction est punie de cinq ans d’emprisonnement;

7° Il est porté au double lorsque l'infraction est punie de trois ans d'emprisonnement au plus.

Les dispositions du présent article ne sont toutefois pas applicables à l'auteur ou au complice de l'infraction qui, à la demande des autorités judiciaires ou administratives, leur a remis la version en clair des messages chiffrés ainsi que les conventions secrètes nécessaires au déchiffrement.”

Verstößt eine gesetzliche Pflicht zur Herausgabe von Schlüsseln und Passwörtern gegen das Aussageverweigerungsrecht des Beschuldigten aus dem nemo-tenetur-Grundsatz, stellt auch die Sanktionierung der Wahrnehmung des Aussageverweige-

um ein Verbrechen oder Vergehen zu begehen oder vorzubereiten oder um die Vorbereitung oder die Begehung zu erleichtern, wird die Obergrenze der Freiheitsstrafe wie folgt erhöht:
1. es wird erhöht auf lebenslängliche Freiheitsstrafe, soweit die Tat mit 30 Jahren Freiheitsstrafe bestraft wird;
2. es wird erhöht auf 30 Jahre Freiheitsstrafe, soweit die Tat mit 20 Jahren Freiheitsstrafe bestraft wird;
3. es wird erhöht auf 20 Jahre Freiheitsstrafe, soweit die Tat mit 15 Jahren Freiheitsstrafe bestraft wird;
4. es wird erhöht auf 15 Jahre Freiheitsstrafe, soweit die Tat mit 10 Jahren Freiheitsstrafe bestraft wird;
5. es wird erhöht auf 10 Jahre Freiheitsstrafe, soweit die Tat mit 7 Jahren Freiheitsstrafe bestraft wird;
6. es wird erhöht auf 7 Jahre Freiheitsstrafe, soweit die Tat mit 5 Jahren Freiheitsstrafe bestraft wird;
7. es wird erhöht auf das Doppelte, soweit die Tat mit 3 Jahren oder mehr Freiheitsstrafe bestraft wird.
Die Regelungen dieses Artikels sind jedoch nicht anwendbar auf einen Täter oder Tatbeteiligten, der den Justiz- oder Verwaltungsbehörden auf deren Aufforderung den Klartext der verschlüsselten Nachricht und die geheimen Vereinbarungen, die für eine Entschlüsselung erforderlich sind, bereitstellt.“

rungsrechts durch den Beschuldigten – hier im Wege einer Strafrahmenerhöhung – einen Verstoß gegen den nemo-tenetur-Grundsatz dar.[1220]

B. Herausgabepflicht privater Dritter (insbes. Systemadministratoren)

Da der Beschuldigte nicht zur Herausgabe verwendeter Schlüssel und Passwörter verpflichtet werden kann, kommen nur dritte, selbst nicht verdächtige Personen als Auskunftspersonen in Betracht. Hierbei ist insbesondere an den jeweiligen Systemadministrator zu denken.[1221]

Dritte Personen können grundsätzlich als Zeugen vernommen werden. Jenseits von Zeugnisverweigerungsrechten unterliegen Zeugen der Aussage- wie der Wahrheitspflicht.[1222] Die Aussagepflicht umfasst aber immer nur eigenes Wissen und eigene Wahrnehmungen des Zeugen, er muss sich nicht erst Wissen verschaffen.[1223] Kennt eine dritte Person also Passwörter oder Schlüssel, ist sie als Zeuge verpflichtet, diese preiszugeben. Weiß der Zeuge aber nur, wo entsprechende Schlüssel gespeichert sind, verpflichtet ihn die allgemeine Zeugenpflicht nicht dazu, die Daten selbst zu finden, zu sortieren oder aufzubereiten.[1224]

Derartige Pflichten könnten sich aber aus der Editionspflicht des § 95 I StPO, die auch Zeugen trifft, ergeben. Die Vorlageverpflichtung aus § 95 I StPO richtet sich allerdings immer nur an den Gewahrsamsinhaber. Gewahrsam liegt im strafrechtlichen Sinne vor bei Bestehen eines tatsächlichen Herrschaftsverhältnisses, das von einem Herrschaftswillen getragen wird. Kann der Administrator tatsächlich auf Daten zugreifen und diese entschlüsseln, dürfte regelmäßig (Mit-)Gewahrsam vorliegen.[1225] Die Editionspflicht ist dabei in ihrer Reichweite akzessorisch zum Durchsuchungsbeschluss: Voraussetzung für eine Editionspflicht ist also, dass die Daten lokal oder in anderen, ebenfalls vom Durchsuchungsbeschluss umfassten Räumlichkeiten gespeichert sind.[1226] Die Durchsuchung externer Datenbestände ist ausgeschlossen. Befinden sich die externen Datenbestände im Inland, kommt jedoch eine entsprechende Erweiterung der Durchsuchungsanordnung bei Gefahr im Verzug

1220 So auch *Baum/Trafkowski,* CR 2002, 69, 71.

1221 *Bär*, Handbuch zur EDV-Beweissicherung, S. 399. Vgl. daneben ausführlich *Radtke*, Aktive Mitwirkungspflichten und die "freiwillige" aktive Mitwirkung des Betroffenen bei dem Zugriff auf elektronisch gespeicherte Daten im Strafprozess, in: *Eser/Goydke/Maatz/Meurer,* Strafverfahrensrecht in Theorie und Praxis, S. 321, für die zunehmende Praxis der Strafverfolgungsbehörden, Banken hinsichtlich Beweisen für Steuerhinterziehungen ihrer Kunden sowie dazu geleisteter Beihilfe durch Bankmitarbeiter zu durchsuchen. Einen Überblick über die Mitwirkungspflichten von Zeugen gibt auch *Gercke*, Telekommunikationsüberwachung (TKÜ), in: *Roggan/Kutscha,* Handbuch zum Recht der Inneren Sicherheit, S. 146, 166 f.

1222 *Bär*, Handbuch zur EDV-Beweissicherung, S. 442.

1223 *Bär*, Handbuch zur EDV-Beweissicherung, S. 443.

1224 *Bär*, Handbuch zur EDV-Beweissicherung, S. 444.

1225 Ähnlich auch *Bär*, Handbuch zur EDV-Beweissicherung, S. 449.

1226 Ausführlich dazu *Bär,* CR 1995, 158-169, 227-234 228 f.

nach § 105 I StPO durch den Staatsanwalt in Betracht. Für externe Daten auf ausländischen Rechnern scheidet dieses Vorgehen allerdings aus.[1227]

Im Ergebnis ist festzuhalten, dass bereits de lege lata eine gesetzliche Verpflichtung Dritter zur Herausgabe von Schlüsseln und Passwörtern besteht.

C. Herausgabepflicht von Diensteanbietern

Daneben sind auch Telekommunikationsdiensteanbieter zur Zusammenarbeit mit staatlichen Sicherheitsbehörden verpflichtet. In Fällen angeordneter Telekommunikationsüberwachung (nach der StPO, dem G10, dem Zollfahndungsdienstgesetz, dem BKA-Gesetz oder nach Landesrecht) sind die Diensteanbieter nach § 8 III S. 1 TKÜV verpflichtet, Schlüssel und Passwörter bei netzseitig verschlüsselter Telekommunikation ebenfalls zu speichern und den Sicherheitsbehörden bereitzustellen:

> „§ 8 III TKÜV: Wenn der Verpflichtete die ihm zur Übermittlung anvertraute Telekommunikation netzseitig durch technische Maßnahmen gegen unbefugte Kenntnisnahme schützt, hat er die von ihm für diese Telekommunikation angewendeten Schutzvorkehrungen bei der an dem Übergabepunkt bereitzustellenden Überwachungskopie aufzuheben. Satz 1 gilt entsprechend bei der Anwendung von Komprimierungsverfahren. […]"

Dabei geht es aber immer nur um Verschlüsselung, die *durch den Diensteanbieter selbst* vorgenommen wird. Insoweit handelt es sich *nicht* um eine Lösung des hier diskutierten Problems der fehlenden Kenntnisnahmemöglichkeit bei teilnehmerautonomer Verschlüsselung. Auch fällt Internet-Telefonie bislang nicht[1228] unter diese Regelungen und soll es wohl auch in Zukunft nicht.[1229] Schließlich bestehen erhebliche Bedenken hinsichtlich der Verfassungsmäßigkeit von § 8 III S. 1 TKÜV, da die

1227 Vgl. die Problemdarstellung auch unter Thematisierung der völkerrechtlichen Implikationen bei *Bär,* CR 1995, 158-169, 227-234, 232. *Bär* geht im Ergebnis davon aus, dass eine derartige grenzüberschreitende Online-Ermittlung gegen das völkerrechtliche Territorialprinzip verstoßen würde, was zu einem Beweisverwertungsverbot führen würde.

1228 Wie sich aus der Diskussion um die Quellen-TKÜ und aus Presseberichten ergibt: heise online vom 13.02. 2009, Bericht: NSA bietet Milliarden, um Skype abzuhören, verfügbar unter: http://www.heise.de/newsticker/Bericht-NSA-bietet-Milliarden-um-Skype-abzuhoeren--/meldung/132502 (27.03.2009); heise online vom 23.02. 2009, Europäische Strafermittler wollen VoIP-Gespräche abhören können, verfügbar unter: http://www.heise.de/newsticker/Europaeische-Strafermittler-wollen-VoIP-Gespraeche-abhoeren-koennen--/meldung/133343 (27.03. 2009).

1229 So hinsichtlich des Umgangs mit der Verschlüsselung von Skype laut heise online vom 05. 12.2007, VoIP-Überwachung respektiert Verschlüsselung, verfügbar unter: http://www.heise.de/newsticker/VoIP-Ueberwachung-respektiert-Verschluesselung--/meldung/100072 (27.03. 2009) explizit BKA-Chef Ziercke: „Ich kann mir nicht vorstellen, dass der Provider darauf eingehen würde, und ich will es auch gar nicht, um es ganz klar zu sagen, weil ich glaube, dass ganz grundsätzlich erst einmal anerkannt werden muss, dass Electronic Banking und der Finanzstrom in Datennetzen natürlich sicher sein muss. Dazu ist Verschlüsselung und Kryptografie gedacht. Deshalb macht es auch keinen Sinn, zu verlangen, der Kryptoschlüssel müsste irgendwo hinterlegt werden bei der Zentrale, das wollen wir nicht. Deshalb ist unser Ansatz ein anderer, dass wir vor oder nach der Verschlüsselung ansetzen."

Telekommunikationsdiensteanbieter durch die Speicherungsverpflichtung zu höchst sicherheitsempfindlichen Stellen werden.[1230]

Gleichwohl gehen die politischen Tendenzen derzeit in Richtung der Förderung von Verschlüsselung durch Diensteanbieter und nicht durch den Nutzer selbst – wie der geplante sichere Bürger-E-Mail-Dienst De-Mail[1231] zeigt: die gesamten Sicherheitsmechanismen sollen dabei

> „beim Provider im Hintergrund ablaufen, um die Nutzung so einfach wie möglich zu machen. So sei dort etwa eine Kontrolle auf Schadsoftware und eine Versandberechtigung, die Integritätssicherung über eine Prüfsumme, die Verschlüsselung über S/MIME und eine Ergänzung von Metadaten durchzuführen.“[1232]

Es ist denkbar, dass nach Etablierung der De-Mail-Dienste diese zur Speicherung der verwendeten Schlüssel verpflichtet werden sollen – wobei eine zusätzliche teilnehmerautonome Verschlüsselung zwar möglich, aber jedenfalls zur Kommunikation mit Behörden nicht geeignet sein dürfte. Die staatliche Gewährleistung vertraulicher E-Mail-Kommunikation könnte die zunehmende Verbreitung teilnehmerautonomer Verschlüsselung zwar stoppen. Gerade die Kommunikationsteilnehmer, denen das sicherheitsbehördliche Interesse gilt, werden aber weiterhin auf teilnehmerautonome Verschlüsselung setzten, so dass eine Herausgabepflicht der Diensteanbieter von Passwörtern und Schlüsseln hier gerade nicht die sicherheitsbehördlichen Kenntnisnahmeoptionen absichern kann.

D. Ergebnis

Eine gesetzliche Verpflichtung zur Herausgabe von verwendeten Schlüsseln oder Passwörtern *gegenüber Beschuldigten* wäre ein Verstoß gegen den nemo-tenetur-Grundsatz und daher *verfassungswidrig*.

Dritte (nicht beschuldigte) Personen sind dagegen *bereits nach geltender Rechtslage* als Zeugen *verpflichtet*, Passwörter zu nennen und Daten in ihrem Gewahrsam

1230 Es handelt sich um ein relatives Verschlüsselungsverbot in Form des *`key escrow´*-Modells. Siehe dazu Teil 4, insbesondere zu Fragen der Verhältnismäßigkeit im engeren Sinne unter A.I.3.c.dd).

1231 Siehe Einzelheiten dazu bei heise online vom 17.11.2008, Bundesregierung verteidigt Projekt für sichere Bürger-E-Mail, verfügbar unter: http://www.heise.de/newsticker/Bundesregierung-verteidigt-Projekt-fuer-sichere-Buerger-E-Mail--/meldung/119004 (27.03.2009) und heise online vom 07.01.2009, Bürger-E-Post De-Mail soll "geprüfte statt geglaubte Sicherheit" bringen, verfügbar unter: http://www.heise.de/newsticker/Buerger-E-Post-De-Mail-soll-gepruefte-statt-geglaubte-Sicherheit-bringen--/meldung/121274 (27.03.2009). Vgl. den Entwurf eines Gesetzes zur Regelung von Bürgerportalen und zur Änderung weiterer Vorschriften vom 20.02.2009, BT-Drs. 174/09 sowie unten in Teil 7 unter B.

1232 heise online vom 17.11.2008, Bundesregierung verteidigt Projekt für sichere Bürger-E-Mail, verfügbar unter: http://www.heise.de/newsticker/Bundesregierung-verteidigt-Projekt-fuer-sichere-Buerger-E-Mail--/meldung/119 004 (27.03.2009).

herauszugeben. Letzteres bedeutet praktisch nichts anderes als Entschlüsselung der Daten oder Herausgabe der verwendeten Schlüssel.

Diensteanbieter sind zwar nach aktueller Rechtslage zur Herausgabe von Passwörtern und Schlüsseln *verpflichtet*. Dabei kann es sich aber immer *nur um von den Diensteanbietern selbst verwendete oder angebotene Verschlüsselungsverfahren* handeln. Das Dilemma der teilnehmerautonomen Verschlüsselung, dem diese Arbeit gilt, wird davon nicht berührt.

Teil 6: Grundrecht auf Verschlüsselung als staatliche Schutzpflichterfüllung?

Ein Grundrecht auf Verschlüsselung liegt aber nicht nur dann vor, wenn ein Verschlüsselungsverbot nicht in verfassungsgemäßer Weise eingeführt werden könnte. Von einem Grundrecht auf Verschlüsselung kann man auch sprechen, wenn sich eine positive Verpflichtung, Daten zu verschlüsseln, aus den Grundrechten ergeben würde. Angesprochen sind damit die objektiv-rechtlichen Grundrechtsgehalte jenseits der klassischen abwehrrechtlichen Dimension der Grundrechte, insbesondere die Schutzpflichten:

> „Grundrechtliche Schutzpflichten sind Pflichten des Staates, grundrechtsbewehrte Rechtsgüter seiner Bürger zu schützen."[1233]

Zur Veranschaulichung dient folgendes

Szenario 4
Staat S verschlüsselt Daten nicht.

Dabei kann innerhalb dieses Szenarios weiter unterschieden werden: Muss der Staat eigene Daten (d.h. hier rein staatliche Daten ohne konkreten Bezug zu einer bestimmten oder bestimmbaren Person) verschlüsseln? Muss der Staat Daten mit einem derartigen Personenbezug verschlüsseln? Weitere Anforderungen könnten sich bei staatlichen E-Government-Anwendungen ergeben: Welche Sicherheitsvorkehrungen verlangen solche staatlichen Angebote? Ergeben sich dabei abweichende Beurteilungen je nachdem, ob die Nutzung von E-Government-Angeboten freiwillig erfolgt oder ob der Staat diese verpflichtend vorschreibt (wie etwa bei der Umsatzsteuervoranmeldung[1234])?

Es kann also jeweils nach verschiedenen Kriterien kategorisiert werden: Zum einen nach der Betroffenheit (Daten einer bestimmten Person oder staatliche Daten ohne Personenbezug); zum anderen nach der Schutzrichtung (Transportsicherheit oder Vertraulichkeitsschutz) und zuletzt nach der Eigenverantwortung des Nutzers

1233 *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 20.

1234 Vgl. § 18 Umsatzsteuergesetz i.d.F. vom 22.09.2005 (BGBl. I S. 386): „[Besteuerungsverfahren] (1) Der Unternehmer hat bis zum 10. Tag nach Ablauf jedes Voranmeldungszeitraums eine Voranmeldung nach amtlich vorgeschriebenem Vordruck auf elektronischem Wege nach Maßgabe der Steuerdaten-Übermittlungsverordnung zu übermitteln, in der er die Steuer für den Voranmeldungszeitraum (Vorauszahlung) selbst zu berechnen hat; auf Antrag kann das Finanzamt zur Vermeidung von unbilligen Härten auf eine elektronische Übermittlung verzichten."

(freiwillige oder verpflichtende Nutzung). Daraus könnte man etwa folgende paradigmatische Unterszenarien bilden:[1235]

Unterszenario 4a
Staat S verschlüsselt eigene Daten ohne Personenbezug nicht.

Unterszenario 4b
Staat S verschlüsselt Daten von Personen nicht.

Unterszenario 4c
Staat S verschlüsselt Daten von Personen im Rahmen von E-Government-Anwendungen nicht.

Diese Szenarien nehmen die grundrechtlichen Anforderungen an Regelungen für den Umgang staatlicher Stellen mit Daten in den Blick – angesichts der von Dritten (Hacker etc.) oder der Technologie (E-Mail- und Internet-Protokolle) selbst ausgehenden Gefahren oder Bedrohungen.

Staatliche Schutzpflichterfüllung kann aber auch die Schaffung von Regelungen hinsichtlich des Verhaltens von Dritten implizieren. Es ist zu untersuchen, inwiefern der Staat aus Schutzpflichtaspekten verpflichtet sein könnte, Dritte zum Schutz der Daten der Grundrechtsberechtigen zu verpflichten – insbesondere durch Verschlüsselung. Dem entspricht

Szenario 5
Staat S verpflichtet Dritte nicht dazu, Daten zu verschlüsseln.

Wie bisher ist bei den Szenarien 4 und 5 zunächst an Verschlüsselung zum Privatsphärenschutz (A.) zu denken. Daneben dient Verschlüsselung auch der wirtschaftlichen Entfaltungsfreiheit (B.). Hinsichtlich der Verschlüsselung von Daten

1235 Diese sollen aber an dieser Stelle nur zur weiteren Verdeutlichung dienen; sie sind für eine weitere, anhand dieser Unterszenarien differenzierten Untersuchung nicht tauglich: Zum einen sind die Unterszenarien nicht wirklich trennscharf (wie man schon an der Formulierung von Unterszenario 4b bemerkt, das nach seinem Wortlaut ja ohne Weiteres das Unterszenario 4c umfasst). Die Herstellung der notwendigen Diversifizierung würde demgegenüber zu derart vielen Unterszenarien führen, dass dies weder der Strukturierung des Themas noch der Gesamtschau dienlich wäre. Schließlich ergeben sich in der Sache nicht derartig viele Unterschiede, dass eine Aufteilung notwendig erschiene. Zuletzt sind die Fragestellungen auch inhaltlich so verquickt, dass häufig aus einer Feststellung die nächste (fast) zwangsläufig folgt. Stellt man etwa die Notwendigkeit eines besonderen Vertraulichkeitsschutzes für bestimmte Daten fest, sind Konstellationen, in denen sich daraus nicht automatisch ergibt, dass bei besonderen Vertraulichkeitsanforderungen natürlich auch die Transportsicherheit entsprechend gewährleistet sein muss, nur schwer denkbar. Eine Aufspaltung in unterschiedliche Szenarien würde nur zu vielerlei Wiederholungen führen. Abweichende Beurteilungen im Einzelfall können dagegen im jeweiligen Kontext dargestellt werden ohne Struktur, Übersichtlichkeit und Lesbarkeit merklich zu beeinträchtigen. Daher bleibt es bei einer Ausrichtung der Untersuchung an Szenario 4.

ohne konkreten Bezug zu einzelnen Personen – und damit ohne Grundrechtsbezug – ist schließlich zu untersuchen, ob sich eventuell aus sonstigen Staatsaufgaben oder rechtsstaatlichen Prinzipien Verschlüsselungsgebote ergeben (C.).

A. Verschlüsselung und Privatsphärenschutz

Zu prüfen ist, ob sich aus dem Fernmeldegeheimnis (Art. 10 I GG), dem Recht auf Unverletzlichkeit der Wohnung (Art. 13 I GG) und/oder dem allgemeinen Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG), insbesondere in seinen Ausprägungen als Recht auf informationelle Selbstbestimmung und als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, objektivrechtliche Grundrechtsgehalte ergeben, die den Staat zum Einsatz von Verschlüsselungsverfahren verpflichten können. Dabei ist hier vor allem an staatliche Schutzpflichten zu denken.

I. Staatliche Schutzpflicht aus dem Fernmeldegeheimnis (Art. 10 I GG)?

1. Prüfungsstruktur

Es herrscht weitgehend Einigkeit darüber, dass eine Übertragung der abwehrrechtlichen Prüfungsstruktur nicht in Betracht kommt:[1236]

Dies liegt auf der Hand, da die Schutzpflichtenkonstellation von einer Dreiecksbeziehung zwischen Staat, Störer und Opfer gekennzeichnet ist. Die abwehrrechtliche Prüfungsdogmatik dagegen fokussiert allein das bipolare Verhältnis Staat – Grundrechtsberechtigter. In diesem Falle ist nur danach zu fragen, ob ein bestimmter Eingriff des Staates in Rechtsgüter des Grundrechtsberechtigten verfassungsrechtlich zu rechtfertigen ist, d.h. in der Regel wegen der Verfolgung gewichtigerer Interessen hinzunehmen ist. Im Dreiecksverhältnis steht der Staat dagegen *zwischen* den Rechtspositionen *zweier* Grundrechtsberechtigter: Was dem einen gegeben wird, wird häufig spiegelbildlich dem anderen genommen. Wo der Staat den einen schützt, greift er in die Rechtpositionen des anderen ein.[1237] Die zu treffende Abwägungsentscheidung entwickelt mithin eine um vieles größere Komplexität, da versucht werden muss, die widerstreitenden Rechtsgüter jeweils zu (größtmöglicher) Entfaltung zu bringen.

1236 *Brüning/Helios,* Jura 2001, 155, 161; *Möstl,* DÖV 1998, 1029, 1035; *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 219 ff.; *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 87.

1237 Diesen Aspekt betonend etwa *Wahl/Masing,* JZ 1990, 553, 556 sowie *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 5.

„Der Unterschied zwischen der Pflicht, Eingriffe zu unterlassen, und der Pflicht, dafür zu sorgen, daß Dritte Eingriffe unterlassen, ist so fundamental und folgenreich, daß sich, jedenfalls unter dogmatischen Gesichtspunkten, jede Relativierung der Unterscheidung verbietet."[1238]

a. Keine Zurechnung auf Grund staatlicher Duldung

Die Gegenauffassung[1239] nimmt dagegen im Wege einer Duldungsfiktionen eine Zurechnung des Verhaltens des Störers vor: Nach der grundgesetzlichen Freiheitskonzeption[1240] ist zunächst jedes Verhalten, das nicht verboten ist, als erlaubt anzusehen. Solange das Verhalten eines Störers nicht durch den Staat unterbunden oder verboten werde, müsse der betroffene Grundrechtsinhaber daher die Störung hinnehmen. Bei rechtswidrigen Beeinträchtigungen stehe dem Betroffenen gerichtlicher Rechtsschutz bzw. bei gegenwärtigen rechtswidrigen Angriffen eventuell ein das staatliche Gewaltmonopol durchbrechendes Notwehrrecht offen. Voraussetzung sei aber jeweils eine *rechtswidrige* Beeinträchtigung. Daraus leitet diese in der Literatur vertretene Auffassung ab, dass für nach der aktuellen Rechtslage rechtmäßige Beeinträchtigungen quasi ein generelles Duldungsgebot bestehe:

„Dem liegt folgender Gedankengang zugrunde: jeder Konflikt zwischen Privaten, der zu einer Grundrechtsbeeinträchtigung führt, ist von dem Beeinträchtigten mit rechtlichen Mitteln abwehrbar oder nicht. Gibt die Rechtsordnung dem Betroffenen keine Abwehrmöglichkeit, so liegt darin eine Erlaubnis für den Störer und ein Duldungsgebot an das Opfer."[1241]

Das Unterlassen staatlichen Schutzes wird nicht als (negatives) Unterlassen einer staatlichen Handlung begriffen, sondern als (positive) Entscheidung, keinen Schutz zu gewähren. So wird aus jeder Grundrechtsbeeinträchtigung, gleichgültig, von wem diese herrührt, ein staatlicher Eingriff, da eine vorangegangene staatliche Entscheidung, Schutz für ein Rechtsgut zu gewähren oder nicht, fingiert wird. So wird das mehrpolige Grundrechtsverhältnis von Störer, Opfer und Staat wieder zu einem rein bipolaren Verhältnis zwischen betroffenem Grundrechtsinhaber einerseits und Staat andererseits, welches wieder nach der klassischen abwehrrechtlichen Grundrechtskonzeption begreifbar scheint.

Wie bereits dargestellt bliebe bei der Reduktion einer Schutzpflichtenkonstellation auf das Verhältnis von betroffenem Grundrechtsinhaber und Staat offen, wie und

1238 *Alexy*, Theorie der Grundrechte, S. 415 f.

1239 Aktuell scheint diese Gegenmeinung an Bedeutung eingebüßt zu haben, vgl. daher nur überblicksartig und die Argumentationsstränge zusammenfassend *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 44 ff.; *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 93 ff., *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 118 ff., *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, S. 36 ff. jeweils m.w.N. sowie *Alexy*, Theorie der Grundrechte, S. 416 ff.

1240 D.h. vor allem der abwehrrechtlich geprägten Freiheitskonzeption; *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 2.

1241 So die vor allem von *Schwabe* und *Murswiek* begründete Argumentation zusammenfassend *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 93.

wo die Rechtsposition des Störers berücksichtigt wird. Schließlich ist eine der bedeutsamsten Fragen innerhalb des Bereichs der staatlichen Schutzgewährleistung die, in welchen Fällen und wie der Staat im Einzelnen Schutz gewährleisten muss. Eine pauschale Zurechnung aller Eingriffe Privater in grundrechtlich geschützte Rechtsgüter trägt nichts zur Lösung dieser Fragestellung bei:[1242]

> „Bei näherem Hinsehen, nämlich bei der Frage, warum und in welchem Umfang und mit welcher Folge der Staat sich private Eingriffe zurechnen lassen muß, zeigen sich gerade die verfassungsrechtlichen Lücken, zu deren Ausfüllung die grundrechtliche Schutzpflicht beitragen könnte. Ob die öffentliche Gewalt Grundrechtsbeeinträchtigungen anregen, fördern, genehmigen, zulassen, billigen oder in Kauf nehmen darf, beantwortet sich aus der *vorausliegenden* Frage, ob, wie und in welchem Umfang sie verpflichtet ist, Beeinträchtigungen zu verhindern.“[1243]

Ausgangspunkt einer staatlichen Schutzpflicht ist nicht die Rechtsgutbeeinträchtigung durch Private, sondern die staatliche Verantwortung, die Rechtsgutbeeinträchtigung zu verhindern:[1244]

> „`Damit ist aber die *Pflicht*, die Eingriffe zu unterbinden, der konstruktive Angelpunkt´, und nicht eine vermeintliche Zurechnung der Handlungen Privater.“[1245]

Weiterhin sind auch da weitergehende Schutzpflichten denkbar, wo Abwehransprüche des Grundrechtsinhabers gegen private Störer durchaus bereits bestehen, denn das Bestehen von Abwehrrechten ist nicht gleichbedeutend mit effektivem Grundrechtsschutz.[1246]

b. Eigenständige Schutzpflichtendogmatik

Die Prüfung des Vorliegens einer Schutzpflichtverletzung kann daher nicht anhand der von abwehrrechtlichen Grundrechtsgehalten bekannten Kategorisierungen erfolgen, sondern muss eigenständig erfolgen. Über die Grundzüge der Prüfung einer Schutzpflichtverletzung scheint grundsätzlich Einigkeit zu herrschen; eine derartige Ausdifferenzierung der Prüfungsstruktur wie hinsichtlich der abwehrrechtlichen Dimension hat sie dabei aber – auch in der Rechtsprechung des BVerfG – noch nicht erfahren.[1247] Die Literatur hat dieser Frage vergleichsweise wenig Aufmerksamkeit

1242 *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 47.

1243 *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 96 f.

1244 So setzt etwa auch *Lübbe-Wolff*, Die Grundrechte als Eingriffsabwehrrechte, S. 71 in ihrem Vorschlag eines nicht-traditionellen Eingriffsbegriffs eine staatliche Ingerenz voraus. Das heißt nichts anderes als dass dem Staat aufgrund wertender Betrachtung eine Verantwortung für Rechtsgutbeeinträchtigungen Privater auferlegt wird.

1245 *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 47 unter Zitierung von *Alexy*, Theorie der Grundrechte, S. 417.

1246 So auch *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 96.

1247 In der Hauptsache geht es dabei um die Prüfung der Verhältnismäßigkeit, insbesondere des Untermaßverbots – da dort dem mehrpoligen Grundrechtsverhältnis Rechnung getragen wer-

geschenkt. Soweit in der Literatur Prüfungsstrukturen vorgeschlagen wurden,[1248] wurden diese hier als Orientierung verwendet. Die im Folgenden vorgenommene Gliederung und Abschichtung der relevanten Probleme folgt ansonsten rein pragmatischen Gesichtspunkten und strebt keinesfalls danach, eine allgemein für Schutzpflichtkonstellationen adäquate Lösung zu finden.

Zunächst ist zu prüfen, ob das jeweils geprüfte Grundrecht neben der abwehrrechtlichen auch eine Schutzpflichtkomponente enthält (2). Um eine staatliche Schutzpflicht zu aktivieren, müsste sodann eine Beeinträchtigung der geschützten Rechtsgüter durch Dritte vorliegen (3).[1249] Schließlich ist zu untersuchen, wie, d.h. in welchem Umfang und mit welchem Inhalt, der Staat seiner Schutzverpflichtung nachkommen muss (4).

2. Schutzpflichtdimension des Fernmeldegeheimnisses (Art. 10 I GG)?

Zu prüfen ist zunächst, ob dem Fernmeldegeheimnis (Art. 10 I GG) über den abwehrrechtlichen Gehalt hinaus eine Schutzpflichtdimension zukommt.

a. Schutzpflicht als objektiv-rechtlicher Grundrechtsgehalt?

Mit dem ersten Abtreibungsurteil[1250] 1975 hat das BVerfG ausdrücklich[1251] eine staatliche Schutzpflicht unmittelbar aus dem Grundrecht auf Leben (Art. 2 II S. 1 GG) abgeleitet:

> „Die Pflicht des Staates, jedes menschliche Leben zu schützen, läßt sich deshalb bereits unmittelbar aus Art. 2 Abs. 2 Satz 1 GG ableiten. Sie ergibt sich darüber hinaus auch aus der aus-

den muss. Siehe dazu ausführlich *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 29 sowie unten bei 4.c.

1248 *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 88 ff.; *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 221 ff.; *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 23 ff.; Anregungen gibt auch *Möstl,* DÖV 1998, 1029, 1035.

1249 Die hier unter Ziffer 1 und 2 geprüften Punkte werden in der Literatur häufig gemeinsam unter den Terminus „Tatbestand" gefasst; *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 89; *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 23.

1250 BVerfGE 39, 1 – Schwangerschaftsabbruch I.

1251 Die argumentative Basis des BVerfG, die Wertordnungsrechtsprechung, wurde dagegen schon vorher, vor allem durch das Lüth- sowie das Hochschulurteil (auf welche auch das BVerfG in der Abtreibungsentscheidung ausdrücklich verweist) begründet: „Ebenso richtig ist aber, daß das Grundgesetz, das keine wertneutrale Ordnung sein will, in seinem Grundrechtsabschnitt auch eine objektive Wertordnung aufgerichtet hat und daß gerade hierin eine prinzipielle Verstärkung der Geltungskraft der Grundrechte zum Ausdruck kommt. Dieses Wertsystem, das seinen Mittelpunkt in der innerhalb der sozialen Gemeinschaft sich frei entfaltenden menschlichen Persönlichkeit und ihrer Würde findet, muß als verfassungsrechtliche Grundentscheidung für alle Bereiche des Rechts gelten; Gesetzgebung, Verwaltung und Rechtsprechung empfangen von ihm Richtlinien und Impulse."; BVerfGE 7, 198, 205 – Lüth.

drücklichen Vorschrift des Art. 1 Abs. 1 Satz 2 GG; denn das sich entwickelnde Leben nimmt auch an dem Schutz teil, den Art. 1 Abs. 1 GG der Menschenwürde gewährt."[1252]

Diese Schutzpflichtenrechtsprechung des BVerfG hat in der Literatur weitreichende Zustimmung erfahren,[1253] wenngleich die Begründungen für die Existenz einer Schutzpflichtdimension vielfältig sind.[1254]

aa) Ausdrückliche Schutzaufträge

So wird zum Teil[1255] entscheidend auf den Wortlaut einzelner Grundrechte,[1256] vor allem auf den expliziten Schutzauftrag aus der Menschenwürde (Art. 1 I S. 2 GG) abgestellt:[1257]

Art. 1 I GG [Schutz der Menschenwürde]: „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt."

Diese Argumentation scheint aber umgekehrt auch zur Ablehnung einer umfassenden grundrechtlichen Schutzpflichtdimension herangezogen werden zu können.[1258] Denn der Verfassungsgeber hat ja die Möglichkeit und das eventuelle Erfordernis von Schutzaufträgen zu Gunsten bestimmter Rechtsgüter durchaus erkannt, explizit aber nur zu Gunsten ausgewählter Rechtsgüter vorgesehen.

Grund für das Fehlen einer parallelen Normierung von Schutzaufträgen zu Gunsten anderer grundrechtlich geschützter Rechtsgüter ist aber allein die dogmatisch herausgehobene Stellung der Menschenwürde und ihre besondere Bedeutung: Jeder Eingriff in die Menschenwürde stellt einen Grundrechtsverstoß dar; eine verfassungsrechtliche Rechtfertigung von Eingriffen in die Menschenwürde ist nicht möglich. Daher ist im Menschenwürdebereich keine (dem einfachen Gesetzgeber oder der vollziehenden Behörde zu überlassende) Abwägungsentscheidung zwischen verschiedenen Rechtsgütern zu treffen. Dementsprechend wird aus der Schutzpflicht zu Gunsten der Menschenwürde ein unbedingter Schutz*auftrag* – der dann auch Ein-

1252 BVerfGE 39, 1, 41.

1253 Vgl. *Isensee*, Das Grundrecht auf Sicherheit, insbes. 27 ff.; *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 19, 77 ff.; *Alexy*, Theorie der Grundrechte, S. 410 ff.; *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, insbes. 43 ff. sowie weitere Literaturnachweise auf S. 61 und 62; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, insbes. 29 ff.; *Dreier*, Dimensionen der Grundrechte, insbes. 47 ff.; *Cremer*, Freiheitsgrundrechte, S. 228 ff. sowie *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 8 m.w.N.

1254 Sogar diejenigen Stimmen in der Literatur, die die Eigenständigkeit einer Rechtsfigur „Schutzpflicht" ablehnen (s.o.), sehen den Staat in der Pflicht, Schutz zu gewährleisten – nur wird die Schutzpflicht dabei als Teil der abwehrrechtlichen Perspektive begriffen.

1255 Siehe dazu *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 41 f.; *Cremer*, Freiheitsgrundrechte, S. 232 ff.; *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 23.

1256 Etwa die Schutzaufträge aus Art. 6 I GG und Art. 6 IV GG; weitere Beispiele siehe ausführlich *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 27 f.

1257 Vgl. *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 26 ff. m.w.N.

1258 *Cremer*, Freiheitsgrundrechte, S. 234; ablehnend dazu *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 196.

gang in den Wortlaut von Art. 1 I GG gefunden hat.[1259] Der Schutzauftrag des Art. 1 I S. 2 GG ist im Kern nichts anderes als eine grundrechtliche Schutzpflicht. Eine Ausgestaltung durch den einfachen Gesetzgeber ist aber – ausnahmsweise – nicht mehr erforderlich. Für alle anderen Grundrechte, die nicht absolut wie die Menschenwürde geschützt sind, ist durch die Legislative eine einfachgesetzliche Ausgestaltung des Schutzes bzw. durch die Exekutive eine Abwägungsentscheidung erforderlich. In diesem konkretisierungsbedürftigen Bereich bleibt es bei der Schutz*pflicht* – ohne die Verdichtung zum Schutz*auftrag*.

Insgesamt spricht der Schutzauftrag des Art. 1 I S. 2 GG also für die Existenz grundrechtlicher Schutzpflichten.

bb) Schutz des Menschenwürdekerns

Wo sich aus dem Wortlaut kein ausdrücklicher Schutzauftrag ergibt, ergebe sich dieser nach einer in der Literatur vertretenen Auffassung aus dem Menschenwürdegehalt des jeweiligen Grundrechts und stimme mit diesem überein.[1260] So stellt etwa der Schutz eines Kernbereichs privater Lebensgestaltung einen in der Menschenwürde wurzelnden Aspekt des Grundrechtsschutzes aus Art. 10 I GG, Art. 13 I GG und Art. 2 I GG i.V.m. Art. 1 I GG dar. Nach der Würdekerntheorie ergeben sich staatliche Schutzpflichten nur für diesen Kernbereichsschutz sowie eventuelle weitere Menschenwürdeaspekte in den genannten Privatsphärengrundrechten.

Auch das BVerfG hat in seinem ersten Abtreibungsurteil auf die Menschenwürde Bezug genommen. Im zweiten Abtreibungsurteil[1261] wird diese Bezugnahme sogar noch deutlicher und das BVerfG scheint stärker auf die Menschenwürde als Quelle der Schutzpflicht abzustellen:

> „Ihren Grund hat diese *Schutzpflicht* in Art. 1 Abs. 1 GG, der den Staat ausdrücklich zur Achtung und zum Schutz der Menschenwürde verpflichtet; ihr Gegenstand und – von ihm her – ihr Maß werden durch Art. 2 Abs. 2 GG näher bestimmt."[1262]

cc) Sicherheit als Staatsaufgabe

Daneben argumentiert das BVerfG aber ebenfalls – wie auch häufig in der Literatur – in Anknüpfung an *Hobbes* und *Locke*, mit der Staatsaufgabe Sicherheit:[1263] Da-

1259 So auch *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, S. 66 f.

1260 Vgl. *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 42 ff. m.w.N. Dürig sah nach *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 59. anscheinend nicht nur den Würde- sondern auch den Wesens- oder Menschenrechtsgehalt als geschützt an (wobei er diese Gehalte nach *Dreier*, in: *Dreier,* GG, Art. 1, Rn. 163 als inhaltsgleich ansah).

1261 BVerfGE 88, 203 – Schwangerschaftsabbruch II.

1262 BVerfGE 88, 203, 251.

1263 *Isensee*, Das Grundrecht auf Sicherheit, S. 3 ff.; *Di Fabio*, Risikoentscheidungen im Rechtsstaat, S. 43 ff.; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 37 ff. m.w.N.;

nach verzichtet der Einzelne zu Gunsten des Staates auf die gewaltsame private Durchsetzung seiner Rechte und Interessen. Die Unterwerfung unter ein staatliches Gewaltmonopol setzt aber voraus, dass der Staat im Gegenzug die Sicherheit des Einzelnen gewährleistet:[1264]

> „Doch der Verzicht auf Gewalt ist nicht bedingungslos. Die Unterwerfung steht unter Vorbehalt. Sie gilt nur, solange der Staat willens und mächtig ist, die Sicherheit des Bürgers, den Sinn seiner Existenz, zu gewährleisten. Der Staat, der nicht die Macht besitzt, zu schützen, besitzt auch nicht das Recht, Gehorsam zu verlangen."[1265]

Die Daseinsberechtigung des Staates beruht demzufolge gerade darauf, dass er die Sicherheit des Einzelnen gewährleistet und dessen Rechte schützt.

> „Soll der Staat die Sicherung des inneren und äußeren Friedens gewährleisten, soll er sich also als Friedensordnung ausgestalten, so müsse er zwangsläufig auch aktiven Schutz gewähren."[1266]

Dabei stand der Schutzauftrag des Staates sogar an erster Stelle; ein Bewusstsein für die Notwendigkeit nicht nur von Sicherheit *durch* den Staat, sondern auch *vor* dem Staat, wurde erst von *Locke* entwickelt.[1267] Dogmatischer Anknüpfungspunkt sind dabei die einzelnen Grundrechte, die die generelle Staatsaufgabe Sicherheit konkretisieren sollen.[1268] Auch das BVerfG hat implizit mit seiner Wertordnungsrechtsprechung, zum Teil aber auch explizit auf diese Staatsaufgabenargumentation Bezug genommen:

> „Die Sicherheit des Staates als verfaßter Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit seiner Bevölkerung sind Verfassungswerte, die mit anderen im gleichen Rang stehen und unverzichtbar sind, weil die Institution Staat von ihnen die eigentliche und letzte Rechtfertigung herleitet."[1269]

eine ausführliche Darstellung auch bei *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 148 ff. sowie *Cremer*, Freiheitsgrundrechte, S. 258 ff.

1264 Siehe ausführlich dazu *Isensee*, Das Grundrecht auf Sicherheit, S. 3 ff. m.w.N.; *Roßnagel,* ZRP 1997, 26, 28; *Ronellenfitsch,* DuD 2008, 110, 110; *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 2.

1265 *Isensee*, Das Grundrecht auf Sicherheit, S. 3.

1266 *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 39.

1267 So *Isensee*, Das Grundrecht auf Sicherheit, S. 6; *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 153.

1268 *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 39 f.; *Isensee*, Das Grundrecht auf Sicherheit, S. 33. Damit soll hier noch nicht die Entscheidung vorweggenommen werden, ob es sich bei den Schutzpflichten um eine rein objektiv-rechtliche Grundrechtsdimension im Sinne einer bloßen staatlichen Aufgabe handelt, oder ob sich daraus auch ein subjektivrechtlicher Anspruch des Grundrechtsberechtigten auf staatlichen Schutz ergibt; vgl. zu dieser Trennung von Aufgabe und (Grund-)Recht *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 166 sowie *Cremer*, Freiheitsgrundrechte, S. 245.

1269 BVerfGE 49, 24, 56 f. – Kontaktsperre.

dd) Argumentationslücken

Vollends zu überzeugen vermag weder die ideengeschichtliche Staatsaufgabenargumentation noch die Ableitung von Schutzpflichten über den Menschenwürdegehalt der Grundrechte. Vermag der ideengeschichtliche Ansatz nicht plausibel zu machen, wie aus der objektiven Aufgabe ein subjektives Recht des Grundrechtsberechtigten wird,[1270] kann die Menschenwürdethese logisch konsistent nur Schutzpflichten hinsichtlich der Ausprägungen der Menschenwürde in Spezialgrundrechten erklären, *umfassende* staatliche Schutzpflichten ergeben sich daraus nicht.[1271]

Gleichwohl entspricht das Ergebnis – die Annahme einer Schutzpflichtdimension der Grundrechte – nicht nur der ständigen Rechtsprechung des BVerfG sowie mehrheitlich den in der Literatur vertretenen Auffassungen, es scheint vor allem das politisch gewünschte Ergebnis zu sein:[1272] Man will schlicht und einfach die Grundrechtsberechtigten nicht Beeinträchtigungen ihrer Grundrechtspositionen ausliefern, nur weil diese nicht vom Staat, sondern von Privaten ausgehen.

Dem entsprechend wurde von *Isensee*[1273] darauf hingewiesen, dass Freiheit und Sicherheit – oft allein als widerstreitende Interessen wahrgenommen – darüber hinaus auch zwei Aspekte einer einzigen Staatsaufgabe – Rechtsgüterschutz – darstellen und insoweit in einem weitaus komplexeren Zusammenhang stehen:

> „Sicherheit und Freiheit bezeichnen die Unversehrtheit der Rechtsgüter, erstere im Verhältnis zu Privaten, letztere im Verhältnis zur öffentlichen Gewalt. Unter dem ersten Aspekt hat der Staat Übergriffe anderer zu verhindern, unter dem zweiten selbst Übergriffe zu unterlassen. […] Der Schutz des Staates konstituiert den status positivus des Bürgers, die Rechtswahrung den status negativus. Beide status bilden ein integrales Ganzes. Es gibt daher keine Antinomie zwischen den beiden Rechtswerten. Allenfalls ergibt sich eine Spannung im konkreten Fall, die der Gesetzgeber oder der Gesetzanwender auszugleichen hat.“[1274]

ee) „Pervertierung“ der Freiheitsrechte?

Zum Teil wurde gegen die Annahme einer Schutzpflichtdimension der Grundrechte eingewandt, eine solche „pervertiere“ geradezu die Grundrechte in ihrer Primärfunktion als Freiheitsrechte, wenn man sie nun dazu nutze, Eingriffe in die Freiheit zu

1270 So auch *Cremer*, Freiheitsgrundrechte, S. 259.

1271 So auch *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 195: „Soweit also eine Beeinträchtigung der Würde durch Dritte in Rede steht, bedarf es keiner Projektion dieser Schutzpflicht auf die (auch nicht leichter als die Würde zu präzisierenden) Kerngehalte der nachfolgenden Grundrechte. Weder Leben noch Gesundheit sind als solche Bestandteil des Schutzguts Würde und werden somit auch von der Schutzpflicht aus Art. 1 I 2 GG nicht erfaßt.“

1272 Auch *Cremer*, Freiheitsgrundrechte, S. 259 f. spricht insoweit von dem „verbreiteten (verfassungspolitischen) Wunsch nach verfassungsrechtlichem Schutz des Einzelnen gegenüber privaten Übergriffen“.

1273 *Isensee*, Das Grundrecht auf Sicherheit, S. 21 ff.

1274 *Isensee*, Das Grundrecht auf Sicherheit, S. 21.

legitimieren – so unter anderem das Sondervotum von *Rupp-von Brünneck* und *Simon* zum ersten Abtreibungsurteil:[1275]

> „Unser stärkstes Bedenken richtet sich dagegen, daß erstmals in der verfassungsgerichtlichen Rechtsprechung eine objektive Wertentscheidung dazu dienen soll, eine Pflicht des Gesetzgebers zum Erlaß von Strafnormen, also zum stärksten denkbaren Eingriff in den Freiheitsbereich des Bürgers zu postulieren. Dies verkehrt die Funktion der Grundrechte in ihr Gegenteil. Wenn die in einer Grundrechtsnorm enthaltene objektive Wertentscheidung zum Schutz eines bestimmten Rechtsgutes genügen soll, um daraus die Pflicht zum Strafen herzuleiten, so könnten die Grundrechte unter der Hand aus einem Hort der Freiheitssicherung zur Grundlage einer Fülle von freiheitsbeschränkenden Reglementierungen werden."[1276]

Dem ist mit *Isensee*[1277] entgegen zu halten, dass auch die Konsequenzen dieser von ihm als „Staatsabwehrdoktrin" bezeichneten Auffassung als „Pervertierung" der Freiheitsrechte begriffen werden könnten: Die Beschränkung der Wirkung der Freiheitsgrundrechte auf das Verhältnis von eingreifendem Staat zu abwehrendem Grundrechtsberechtigten ließe die grundrechtlich geschützten Rechtsgüter des Grundrechtsberechtigten im Verhältnis zu Beeinträchtigungen durch Private ungeschützt.[1278] Ein rein einfachgesetzlicher Schutz des Grundrechtsberechtigten gegenüber dem privaten Störer kann in dieser Situation nicht für angemessenen Ausgleich sorgen. Eine solche unterverfassungsrechtliche Norm würde sich gegenüber dem Störer als Grundrechtseingriff – in jedem Falle in die allgemeine Handlungsfreiheit (Art. 2 I GG) – darstellen, der verfassungsrechtlich gerechtfertigt sein müsste. Hier würden also die Grundrechte des Störers Berücksichtigung finden. Ohne eine grundrechtliche Schutzpflicht (sei sie nun als subjektives Recht durchsetzbar oder eine rein objektiv-rechtlich bestehende Grundrechtsdimension) würde für die Rechtsposition des Betroffenen keine vergleichbare verfassungsrechtliche Rechtsposition streiten.[1279] Unter Umständen kann aber nur eine solche bei einer Abwägung mit den verfassungsrechtlich geschützten Rechten des Störers berücksichtigt werden. Offensichtlichstes Beispiel dafür sind Grundrechte, für die nur die verfassungsimmanenten Schranken gelten – wie etwa die Religionsfreiheit (Art. 4 I GG). Aber auch im Übrigen müsste gleichermaßen eine verfassungsrechtlich privilegierte Rechtspositi-

1275 BVerfGE 39, 1, 68 ff.

1276 BVerfGE 39, 1, 73.

1277 *Isensee*, Das Grundrecht auf Sicherheit, S. 31 ff.

1278 So *Isensee*, Das Grundrecht auf Sicherheit, S. 32: „Eine grundrechtliche Freiheit, die den Schutz der öffentlichen Gewalt abwiese, fiele der privaten Gewalt anheim."

1279 Dabei ist weiter zu bedenken, dass es sich bei den meisten Zwecken, die Grundrechtseingriffe rechtfertigen können, etwa die öffentliche Sicherheit oder eine effektive Strafverfolgung, nur scheinbar um rein öffentliche Interessen handelt. Wie *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 202 ff. zusammenfassend schön darstellt, stehen hinter den vermeintlich öffentlichen Interessen zunächst private Interessen, etwa Schutz von Leben und Gesundheit. Die Abgrenzung zwischen öffentlichen und privaten Interessen verläuft keineswegs klar.

on für den betroffenen Grundrechtsberechtigten wie für den privaten Störer streiten, soll letzterer nicht gegenüber ersterem bevorzugt werden:[1280]

> „Die Lücke könnte auch nicht durchgehend über die einfachen Gesetze, etwa die Straf- oder Polizeigesetze, geschlossen werden, weil diese aus sich heraus, ohne Rückhalt in der Verfassung, verfassungsrechtliche Freiheitsrechte nicht einschränken könnten. Grundrechte denaturierten unter diesen Bedingungen zu Privilegien des Rechtsbrechers. Nun gehört es zwar zu den unverlierbaren Erkenntnissen der liberal-menschenrechtlichen Tradition, daß *auch* der Störer der Rechtsordnung an den Menschenrechten teilhat. Aber das bedeutet nicht, daß die Menschenrechte *allein* die Rechte des Störers sind, nicht auch die Rechte des Opfers. Für das Opfer jedoch ist kein Platz im Schutzbereich der Grundrechte, wie ihn die Staatsabwehrdoktrin absteckt."[1281]

Angesichts der fortschreitenden Privatisierung von ehemals staatlich wahrgenommenen Aufgaben der Daseinsvorsorge oder Infrastrukturverantwortung (das Post- und Fernmeldegeheimnis des Art. 10 I GG ist hierfür ein Paradebeispiel) gewinnt die Schutzpflichtdimension zusätzlich an Relevanz: Da mit der Privatisierung die unmittelbare Grundrechtsbindung entfällt, wäre der Grundrechtsberechtigte gegenüber den privaten Dienstleistern schutzlos – wenn nicht der Staat im Rahmen seiner Privatisierungsfolgenverantwortung diesen Schutz gewährleistet.

> „Der Übergang von staatlicher Erfüllungsverantwortung zu privatwirtschaftlicher Aufgabenerledigung und der damit einhergehende Fortfall unmittelbarer Grundrechtsbindung aktivieren nämlich die Pflicht des Staates, im Rahmen seiner Privatisierungsfolgenverantwortung die grundrechtlichen Schutzgüter gegen die nunmehr selbst nicht mehr grundrechtsgebundene Wirtschaftstätigkeit zu schützen."[1282]

Dass sich der Staat, wenn er öffentliche Aufgaben erfüllt, nicht der Grundrechtsbindung entziehen kann, zeigt Art. 1 III GG, der Gesetzgebung, vollziehende Gewalt und Rechtsprechung an die Grundrechte bindet, unabhängig von Handlungs- und Rechtsform sowie benutztem Mittel.[1283] Daraus ergibt sich die Privatisierungsfolgenverantwortung. Was ist diese Privatisierungsfolgenverantwortung aber anderes als eine staatliche Schutzpflicht?[1284]

Von einer „Pervertierung" der Freiheitsrechte durch die Annahme einer Schutzpflichtdimension kann daher keine Rede sein, vielmehr spricht die umfassende staatliche Bindung an die Grundrechte gerade *für* eine Schutzpflichtdimension. Schließlich hat *Hermes*[1285] zutreffend darauf hingewiesen, dass die Befürchtung einer „Pervertierung" der Freiheitsrechte auf der falschen Prämisse beruhe, aus einer Schutzpflicht ergebe sich eine zusätzliche Befugnis zum Einschreiten gegen den Störer.

1280 Siehe auch das Beispiel bei *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 205.

1281 *Isensee*, Das Grundrecht auf Sicherheit, S. 32.

1282 *Möstl,* DÖV 1998, 1029, 1030.

1283 *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 1, Rn. 227.

1284 *Möstl,* DÖV 1998, 1029, 1030 spricht insoweit von einer Verstärkung des Schutzpflichtgedankens durch die neuen Formen staatlicher Aufgabenerledigung, insbes. durch Privatisierung; vgl. zum staatlichen Funktionswandel bei der Erfüllung von Staatsaufgaben *Hermes*, Staatliche Infrastrukturverantwortung, S. 236.

1285 *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 206 ff.

Dies ist nicht der Fall. Da der Schutz des Betroffenen nur durch Eingriff in die (wenigstens durch die allgemeine Handlungsfreiheit grundrechtlich geschützten) Rechtspositionen des Störers möglich ist, ist stets eine Rechtsgrundlage erforderlich und insoweit zunächst der Gesetzgeber aufgerufen.[1286] Dieser ist durch Art. 70 ff. GG zur Gesetzgebung befugt, bedarf also keinerlei neuer Befugnisnorm. Inhaltlich ist der Gesetzgeber gleichermaßen durch Art. 1 III GG an die Grundrechte gebunden, muss also die für den Störer streitenden Freiheitsrechte beachten. Die Schutzpflicht gibt mithin keine Eingriffsbefugnis, allenfalls einen Impuls zu gesetzgeberischem Tätigwerden.

ff) Ergebnis

Somit ist grundsätzlich eine Schutzpflichtdimension als objektiv-rechtlicher Grundrechtsgehalt zu bejahen:

> „Nach der ständigen Rechtsprechung des Bundesverfassungsgerichts enthalten die Grundrechtsnormen nicht nur subjektive Abwehrrechte des Einzelnen gegen den Staat, sondern sie verkörpern zugleich eine objektive Wertordnung, die als verfassungsrechtliche Grundentscheidung für alle Bereiche des Rechts gilt und Richtlinien und Impulse für Gesetzgebung, Verwaltung und Rechtsprechung gibt. Ob und gegebenenfalls in welchem Umfang der Staat zu rechtlichem Schutz des werdenden Lebens von Verfassungs wegen verpflichtet ist, kann deshalb schon aus dem objektiv-rechtlichen Gehalt der grundrechtlichen Normen erschlossen werden.“[1287]

b. Schutzpflicht aus dem Fernmeldegeheimnis (Art. 10 I GG)?

Zu prüfen ist, ob sich konkret auch aus dem Fernmeldegeheimnis (Art. 10 I GG) eine staatliche Schutzpflicht ergibt. Der Fokus der Schutzpflichtenrechtsprechung des BVerfG, aber auch der Auseinandersetzung in der Literatur, lag häufig auf dem Schutz von Leben und körperlicher Unversehrtheit (Art. 2 II S. 1 GG), da die Schutzpflichtenrechtsprechung hier ihren Ausgang nahm.[1288]

aa) Besonders deutlicher personaler Bezug

Zum Teil wird in der Literatur[1289] erneut an die explizite Schutzpflicht des Art. 1 I S. 2 GG und die daraus abgeleitete Begründung für die Existenz von Schutzpflichten

1286 *Groß,* JZ 1999, 326, 331.
1287 BVerfGE 39, 1 41 f.
1288 Siehe nur *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 2 und 190 ff. sowie BVerfGE 39, 1 – Schwangerschaftsabbruch I.
1289 *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 196 ff.

angeknüpft und so das Erfordernis eines „besonders deutlichen personalen Bezug[s]“[1290] abgeleitet. Schutzpflichten ergeben sich danach aus einer besonderen Nähe zur Menschenwürde und werden für die engere persönliche Lebenssphäre im Rahmen von Art. 2 I GG (also wohl für das allgemeine Persönlichkeitsrecht), für das Recht auf Leben und körperliche Unversehrtheit (Art. 2 II S. 1 GG), die Religionsfreiheit (Art. 4 I GG), das Brief-, Post- und Fernmeldegeheimnis (Art. 10 I GG) und das Recht auf Unverletzlichkeit der Wohnung (Art. 13 I GG) anerkannt.[1291]

bb) Unterscheidung von Zustands- und Besitzstandsverbürgungen sowie Handlungsfreiheitsverbürgungen

Andere Stimmen in der Literatur wollen zwischen Grundrechten, die Zu- oder Besitzstände verbürgen, und solchen, die Handlungsfreiheiten verbürgen, unterscheiden.[1292] Demzufolge könne nicht aus der Existenz eines Grundrechts auch auf die Existenz einer entsprechenden Schutzpflicht geschlossen werden.[1293] Schutzpflichtfähig seien primär solche Rechte, die einen Bestand an Rechtsgütern garantieren, wie etwa das Leben oder das Eigentum. Rechte, die Handlungsfreiheiten verbürgen, wie etwa die Meinungsfreiheit oder das Recht auf Freizügigkeit, garantierten keinen Bestand und seien „kaum“ schutzpflichtfähig, allenfalls hinsichtlich des Schutzes der Voraussetzungen ihrer Ausübung.[1294]

cc) Untrennbarkeit von Individual- und Kollektivrechtsgütern

Das BVerfG hat dagegen für viele Einzelgrundrechte eine Schutzpflichtdimension positiv anerkannt und bisher in keinem Fall eine Schutzpflichtdimension abgelehnt.[1295] Dabei wurde deutlich, dass eine Unterscheidung nach Zustands- oder Be-

1290 *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 196.

1291 *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 198, der sich allerdings, wie sich bereits aus dem Titel seiner Arbeit ergibt, auf die Untersuchung von Schutzpflichten aus Art. 2 II S. 1 GG beschränkt, so dass der Begründung einer Schutzpflichtdimension anderer Grundrechte wohl weniger Interesse galt.

1292 *Gusy,* DÖV 1996, 573, 577.

1293 *Gusy,* DÖV 1996, 573, 578.

1294 *Gusy,* DÖV 1996, 573, 577.

1295 So *Böckenförde,* Der Staat 1990, 1, 7 m.v.w.N.; *Cremer*, Freiheitsgrundrechte, S. 229 weist allerdings darauf hin, dass das BVerfG die Frage nach einer Schutzpflichtdimension von Art. 8 GG im Brokdorf-Beschluss (BVerfGE 69, 315) ausdrücklich offen gelassen habe. Dem kann so nicht gefolgt werden. Das BVerfG hat vielmehr auch für Art. 8 GG eine Schutzpflichtdimension gesehen, daraus nur für den zu entscheidenden Fall keine Anforderungen an die inhaltliche Gestaltung einer Versammlung abgeleitet: „Es bestehen keine Bedenken, diese Rechtsprechung auch auf die Versammlungsfreiheit anzuwenden, zumal dieses Grundrecht auch einen wesentlichen verfahrensrechtlichen und organisationsrechtlichen Gehalt hat; als Freiheitsrecht enthält es keine Aussagen zur inhaltlichen Gestaltung von Versammlungen und

sitzstandsschutz einerseits und Handlungsfreiheitsschutz andererseits wohl keine Stütze in der Rechtsprechung des BVerfG findet. Dieses hatte etwa in der Hochschulentscheidung für die Wissenschaftsfreiheit (Art. 5 III S. 1 GG) sowohl deren Bedeutung für die Selbstverwirklichung des Einzelnen (Handlungsfreiheit) als auch die gesellschaftliche Bedeutung der Institution eines funktionierenden Wissenschaftsbetriebs (Zustandsschutz) betont.[1296] Ähnliches kann auch z.B. für die Rundfunkfreiheit (Art. 5 I S. 2, 2. Alt. GG) konstatiert werden: Diese vereinigt nach dem BVerfG ebenfalls eine Komponente des Zustandsschutzes (Schutz der Institution Rundfunk) mit Handlungsfreiheitsschutz (Schutz der Meinungsbildungsfreiheit).[1297]

Danach scheidet das Kriterium eines besonderen personalen Bezugs zur Begründung einer Schutzpflichtdimension aus. Wie die genannten Entscheidungen des BVerfG deutlich machen, mag zwar der Schutzpflichtbegründung in der Tat stets ein personaler Bezug zu Grunde liegen, dieser muss aber gerade nicht ein „besonderer" sein, vielmehr reichen auch entferntere Bezüge zu Individualrechtsgütern. So wird mittelbar die individuelle Möglichkeit zur Meinungsbildung dadurch geschützt, dass mit der objektiven Rundfunkordnung Meinungsvielfalt gewährleistet wird. Der personale Bezug in der extensiven Betrachtungsweise des BVerfG bietet für Differenzierungsentscheidungen somit keine Handhabe.[1298]

Aufzügen, sondern überläßt diese der freien Selbstbestimmung der Veranstalter und begnügt sich mit organisatorischen Vorgaben für die Durchführung."; BVerfGE 69, 315, 355 f.

1296 Vgl. BVerfGE 35, 79, 113 – Hochschulurteil: „Eine solche Wertentscheidung enthält auch Art. 5 Abs. 3 GG. Sie beruht auf der Schlüsselfunktion, die einer freien Wissenschaft sowohl für die Selbstverwirklichung des Einzelnen als auch für die gesamtgesellschaftliche Entwicklung zukommt. Diese Wertentscheidung bedeutet nicht nur die Absage an staatliche Eingriffe in den zuvor gekennzeichneten Eigenbereich der Wissenschaft; sie schließt vielmehr das Einstehen des Staates, der sich als Kulturstaat versteht, für die Idee einer freien Wissenschaft und seine Mitwirkung an ihrer Verwirklichung ein und verpflichtet ihn, sein Handeln positiv danach einzurichten, d. h. schützend und fördernd einer Aushöhlung dieser Freiheitsgarantie vorzubeugen."

1297 Siehe BVerfGE 57, 295, 320 – 3. Rundfunkentscheidung: „Freie individuelle und öffentliche Meinungsbildung durch den Rundfunk verlangt zunächst die Freiheit des Rundfunks von staatlicher Beherrschung und Einflußnahme. Insoweit hat die Rundfunkfreiheit, wie die klassischen Freiheitsrechte, abwehrende Bedeutung. Doch ist damit das, was zu gewährleisten ist, noch nicht sichergestellt. Denn bloße Staatsfreiheit bedeutet noch nicht, daß freie und umfassende Meinungsbildung durch den Rundfunk möglich wird; dieser Aufgabe läßt sich durch eine lediglich negatorische Gestaltung nicht gerecht werden. Es bedarf dazu vielmehr einer positiven Ordnung, welche sicherstellt, daß die Vielfalt der bestehenden Meinungen im Rundfunk in möglichster Breite und Vollständigkeit Ausdruck findet und daß auf diese Weise umfassende Information geboten wird. Um dies zu erreichen, sind materielle, organisatorische und Verfahrensregelungen erforderlich, die an der Aufgabe der Rundfunkfreiheit orientiert und deshalb geeignet sind zu bewirken, was Art. 5 Abs. 1 GG gewährleisten will."

1298 Nach der extensiven Betrachtungsweise des BVerfG stehen damit regelmäßig hinter jedem Gemeinwohlbelang zugleich Individualbelange, so dass der von *Gusy,* DÖV 1996, 573, 577 aufgeworfene Kritikpunkt zur ideengeschichtlichen Begründung von Schutzpflichten ins Leere läuft: Nach *Gusy* vermag dieser Ansatzpunkt Schutzpflichten zu Gunsten überindividueller Belange nicht zu erklären. Hält man mit dem BVerfG den mittelbaren Schutz von Individualrechtsgütern über den Schutz von Rechtsgütern, die zunächst als Kollektivrechtsgüter er-

Dies zeigte bereits die Schleyer-Entscheidung des BVerfG:[1299] Das BVerfG bezog damals neben dem konkret bedrohtem Rechtsgut Leben des von der RAF entführten Hanns-Martin Schleyer auch die Schutzpflicht des Staates „gegenüber der Gesamtheit aller Bürger", die eventuell in Zukunft abstrakt in ihrem Leben durch terroristische Erpressungen bedroht sein könnten, in die Abwägung mit ein. Das auf entferntere Individualrechtsgüter gestützte Kollektivrechtsgut konnte nach der Entscheidung des BVerfG den Schutzpflicht-Imperativ des akut bedrohten Individualrechtsguts zu einer bloßen Abwägungsentscheidung des Staates abschwächen.

> „Das Grundgesetz begründet eine Schutzpflicht nicht nur gegenüber dem Einzelnen, sondern auch gegenüber der Gesamtheit aller Bürger. Eine wirksame Wahrnehmung dieser Pflicht setzt voraus, daß die zuständigen staatlichen Organe in der Lage sind, auf die jeweiligen Umstände des Einzelfalles angemessen zu reagieren; schon dies schließt eine Festlegung auf ein bestimmtes Mittel aus. Darüber hinaus kann eine solche Festlegung insbesondere deshalb nicht von Verfassungs wegen erfolgen, weil dann die Reaktion des Staates für Terroristen von vornherein kalkulierbar würde. Damit würde dem Staat der effektive Schutz seiner Bürger unmöglich gemacht. Dies stünde mit der Aufgabe, die ihm durch Art. 2 Abs. 2 Satz 1 GG gestellt ist, in unaufhebbarem Widerspruch."[1300]

Auch wenn die soeben genannte Entscheidung sicherlich vor allem eine politische war, und zwar, sich im Wege des *judicial self-restraint* nicht in die politischen Entscheidungen der Bundesregierung zu mischen, verdeutlicht sie doch, dass das Vorhandensein eines besonderen personalen Bezugs für das BVerfG bedeutungslos ist. Es zählt allein die Betroffenheit von Individualrechtsgütern, mögen diese auch Bestandteil von Rechtsgütern sein, die sich auf den ersten Blick als Kollektivrechtsgüter darstellen.[1301]

dd) Schutzpflichtdimension aller Grundrechte

Es spricht daher vieles dafür, zunächst für jedes Grundrecht auch eine korrespondierende Schutzpflichtdimension anzunehmen.[1302] Die Frage, inwiefern und welche konkreten Handlungsaufträge an den Staat sich daraus dann ergeben,[1303] wird erst durch die Art der Rechtsgutsbeeinträchtigung näher konkretisiert und ist sodann bei Inhalt und Umfang der Schutzpflicht genauer zu prüfen. Eine vorzeitige Verengung der „Schutzpflichtfähigkeit" von Grundrechten ist nicht erforderlich. Inwieweit be-

scheinen, für ausreichend, sind eigentlich keine Kollektivrechtsgüter denkbar, denen nicht irgendwo auch Individualrechtsgüter zu Grunde liegen. Hinter dem Kollektivrechtsgut Umwelt beispielsweise wird so das Individualrechtsgut der körperlichen Unversehrtheit geschützt.

1299 BVerfGE 46, 160 – Schleyer.

1300 BVerfGE 46, 160, 165.

1301 Zu Bedenken hinsichtlich dieser „kollektiven Sicherheitsinteressen" siehe Lepsius, Das Verhältnis von Sicherheit und Freiheitsrechten in der Bundesrepublik Deutschland nach dem 11. September 2001, verfügbar unter: http://www.aicgs.org/documents/lepsius.pdf (04.12.2009), S. 17 f.

1302 *Ronellenfitsch,* DuD 2008, 110, 111.

1303 Was *Gusy,* DÖV 1996, 573, 577 im Kern wohl mit „Schutzpflichtfähigkeit" meinte.

stimmte Ziele überhaupt im Wege von Schutzpflichten erreicht werden können, ist einzig Frage von Inhalt und Umfang der Schutzpflicht.[1304] Daher ist von einer Schutzpflichtdimension aller Grundrechte auszugehen:[1305]

> „Unter `Rechten auf Schutz´ sollen hier Rechte des Grundrechtsträgers gegenüber dem Staat darauf, daß dieser ihn vor Eingriffen Dritter schützt, verstanden werden. Rechte auf Schutz können sehr Unterschiedliches zum Gegenstand haben. Das Spektrum reicht vom Schutz vor Tötungshandlungen urtümlichen Zuschnitts bis zum Schutz vor den Gefahren der friedlichen Nutzung der Atomenergie. Nicht nur das Leben und die Gesundheit sind mögliche Schutzgüter, sondern alles, was unter grundrechtlichen Aspekten schutzwürdig ist: z.B. die Würde, die Freiheit, die Familie und das Eigentum.“[1306]

Somit kommt auch dem Fernmeldegeheimnis (Art. 10 I GG) eine Schutzpflichtdimension zu, wie das BVerfG ausdrücklich festgestellt hat:[1307]

> „Art.10 Abs.1 GG begründet nicht nur ein Abwehrrecht gegen die Kenntnisnahme des Inhalts und der näheren Umstände der Telekommunikation durch den Staat, sondern auch einen Auftrag an den Staat, Schutz insoweit vorzusehen, als private Dritte sich Zugriff auf die Kommunikation verschaffen.“[1308]

Dieses Ergebnis ist – insbesondere für das Fernmeldegeheimnis – überzeugend. Das Brief-, Post- und Fernmeldegeheimnis (Art. 10 I GG) schützt die Vertraulichkeit individueller Kommunikation, wo diese wegen der räumlichen Distanz der Kommunikationspartner auf einen Übermittler angewiesen ist.[1309] Der Schutz des Art. 10 I GG richtet sich traditionell gegen staatliche Kenntnisnahme einerseits und Kenntnisnahme durch den eingeschalteten Übermittler andererseits, verfügt also gerade über beide Schutzrichtungen.[1310] Die Privatisierung der einstmals staatlich wahrgenommenen Übermittlertätigkeit hat diese Differenzierung allerdings erst richtig zu Tage gefördert:

1304 Die nach *Gusy,* DÖV 1996, 573, 577 fehlende oder eingeschränkte Schutzpflichtfähigkeit von Handlungsfreiheiten führt hier schlicht dazu, dass der Staat nichts tun muss, außer die Möglichkeit zur Handlungsfreiheit zu erhalten; weitergehender Schutz ist hier schlicht nicht erforderlich.

1305 So auch *Ronellenfitsch,* DuD 2008, 110, 110 f.; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 75, 78; *Roßnagel,* ZRP 1997, 26, 28; *Nitz*, Private und öffentliche Sicherheit, S. 260 ff., 368; *Cremer*, Freiheitsgrundrechte, S. 265 f. mit umfassenden Hinweisen auf weiterführende Literatur. Auch *Isensee*, Das Grundrecht auf Sicherheit, S. 33 sowie *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 86 geht offensichtlich von einer Schutzpflichtdimension aller Grundrechte aus.

1306 *Alexy*, Theorie der Grundrechte, S. 410.

1307 Vgl. zur früheren, weniger eindeutigen Rechtsprechung des BVerfG, in der sich die Annahme objektiv-rechtlicher Gehalte des Fernmeldegeheimnisses bereits abzeichnete *Hadamek*, Art. 10 GG und die Privatisierung der Deutschen Bundespost, S. 94 f.

1308 BVerfG, Beschluss vom. 27.10.2006, Az.: 1 BvR 1811/99, Rn. 13.

1309 S.o. in Teil 3 unter A.I. sowie nochmal *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 15; ebenso *Brüning/Helios,* Jura 2001, 155, 159.

1310 S.o. in Teil 3 unter A.I.3.b.cc)(1) sowie *Brüning/Helios,* Jura 2001, 155, 159.

„Die Privatisierung öffnet jedoch den Blick dafür, daß weniger die staatliche Veranstaltung der Post als vielmehr die Einschaltung eines Vermittlers als solche eine mögliche Gefährdung des Kommunikationsgeheimnisses darstellt."[1311]

Dem Fernmeldegeheimnis (Art. 10 I GG) kommt somit eine Schutzpflichtdimension zu.[1312]

c. Umfang der Schutzpflichtdimension

Die Schutzpflichtdimension gilt vom Umfang her hinsichtlich des gesamten abwehrrechtlichen Schutzbereichs: Ist der Schutzbereich eines Grundrechts in einer abwehrrechtlichen Perspektive eröffnet, existiert auch eine entsprechende Schutzpflichtdimension.[1313]

„Die personale und die räumliche Reichweite der Grundrechte als Abwehrrechte entspricht ihrer Reichweite in der Schutzpflichtdimension."[1314]

Auch insoweit erscheint eine Anlehnung an die abwehrrechtliche Grundrechtsdimension angezeigt,[1315] eine nähere Konkretisierung und Begrenzung erfährt die Schutzpflichtdimension bei der Bestimmung ihres Inhalts und Umfangs. Dies entspricht der Herangehensweise der abwehrrechtlichen Perspektive: Zunächst wird das Schutzgut herausgearbeitet (Schutzbereich), erst dann wird in einem zweiten Schritt nach einem möglichen Eingriff gefragt. Der effektive Garantiebereich eines Grundrechts[1316] – also das, was ein Grundrecht tatsächlich am Ende gewährleistet – erschließt sich erst ganz zuletzt bei der Frage, welche Eingriffe verfassungsrechtlich zu rechtfertigen sind und welche nicht. Der vollständige Umfang auch des abwehrrechtlichen Grundrechtsschutzes ergibt sich erst durch eine vollständige Prüfung und nicht schon auf Schutzbereichsebene.

3. Rechtsgutsbeeinträchtigung durch private Dritte

Es müsste eine Beeinträchtigung der grundrechtlich – hier durch das Fernmeldegeheimnis – geschützten Rechtsgüter durch Dritte vorliegen. Dies entspricht dem

1311 *Groß,* JZ 1999, 326, 332.
1312 So auch *Hadamek*, Art. 10 GG und die Privatisierung der Deutschen Bundespost, S. 145.
1313 So auch *Cremer*, Freiheitsgrundrechte, S. 266; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 78; *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 23.
1314 *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 78.
1315 *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 23 sieht den Ausgangspunkt von Abwehr- wie Schutzpflichtdimension in der nach seiner Auffassung objektiv feststellbaren Grundrechtsgewährleistung, die durch das grundrechtliche Schutzgut definiert wird.
1316 Siehe dazu *Lübbe-Wolff*, Die Grundrechte als Eingriffsabwehrrechte, S. 26: „Der *effektive Garantiebereich* ist dagegen derjenige Bereich, in den einzugreifen zugleich eine Verletzung des Grundrechts bedeuten würde, derjenige Teil des Schutzbereichs also, für den die Voraussetzungen der Zulässigkeit von Eingriffen nicht erfüllbar sind."

„Eingriff“ in der abwehrrechtlichen Grundrechtsdimension. Die Schutzpflichtdimension ist demgegenüber dadurch gekennzeichnet, dass die Rechtsgutsbeeinträchtigung (a.) gerade nicht durch den Staat, sondern durch private Störer erfolgt (b.).

a. Rechtsgutsbeeinträchtigung

Es müsste eine Rechtsgutsverletzung vorliegen bzw. die Gefahr einer Rechtsgutsverletzung bestehen.[1317] Das geschützte Rechtsgut stimmt in der abwehrrechtlichen und in der Schutzpflichtdimension überein. Dabei ist nicht nur vor rechtswidrigen Rechtsgutsbeeinträchtigungen Schutz zu gewähren. Rechtmäßig- oder Rechtswidrigkeit der Beeinträchtigung ergeben sich erst durch die grundrechtliche Abwägungsentscheidung.[1318]

aa) Rechtsgut

Das Fernmeldegeheimnis (Art. 10 I GG) schützt die Vertraulichkeit sämtlicher nicht-körperlich übermittelter Individualkommunikation, unabhängig von Übermittlungsart und Ausdrucksform. Dabei werden sowohl unverschlüsselte als auch verschlüsselte Daten geschützt. Schließlich umfasst der Schutzbereich des Fernmeldegeheimnisses auch den Einsatz von Verschlüsselungsverfahren zur Gewährleistung der Vertraulichkeit bei der fernmeldetechnischen Übermittlung. In den Schutzbereich des Fernmeldegeheimnisses fallen mithin alle Formen von individueller Datenkommunikation, sei es per E-Mail, Internettelefonie, Chat etc. Da Daten der Individualkommunikation nicht von solchen der Massenkommunikation ohne inhaltliche Kenntnisnahme zu trennen sind, gilt der Schutz des Fernmeldegeheimnisses umfassend für die gesamte Datenkommunikation.

1317 *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 227 ff.

1318 So auch *Möstl,* DÖV 1998, 1029, 1035, dem dies „eher als ein Aspekt der Reichweite als der Voraussetzungen der Schutzpflicht erscheint.“ Ausführlich dazu auch *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 226 f., der herausarbeitet, dass die Rechtswidrigkeit sich nicht aus einfachgesetzlichen Normen ergeben kann, sondern vielmehr erst Ergebnis einer konkreten Schutzpflichtprüfung ist. Dementsprechend ist die Formulierung des BVerfG, wonach der Staat Schutz vor „rechtswidrigen Eingriffen von Seiten anderer“ (BVerfGE 39, 1, 42 – Schwangerschaftsabbruch I; BVerfGE 40, 160, 164 – Schleyer) zu gewähren hat, weniger als Postulierung der Voraussetzungen einer staatlichen Schutzpflicht zu verstehen, denn als Darstellung des Ergebnisses der Bejahung einer Schutzpflicht.

bb) Verletzungshandlung

Das durch das Fernmeldegeheimnis geschützte Rechtsgut – die Vertraulichkeit nicht-körperlich übermittelter Individualkommunikation – wird dabei vor allem durch Überwachungs- und Abhörmaßnahmen beeinträchtigt. Dabei treten neben staatliche Maßnahmen – etwa Maßnahmen der Telekommunikations- und E-Mail-Überwachung – vor allem Beeinträchtigungen der Vertraulichkeit durch Private.

cc) Gefahr von Rechtsgutsverletzungen

Neben eingetretenen Rechtsgutsbeeinträchtigungen lösen auch drohende Rechtsgutsverletzungen die Schutzpflicht aus.[1319]

> „Daraus können sich verfassungsrechtliche Schutzpflichten ergeben, die es gebieten, rechtliche Regelungen so auszugestalten, daß auch die Gefahr von Grundrechtsverletzungen eingedämmt bleibt. Ob, wann und mit welchem Inhalt sich eine solche Ausgestaltung von Verfassungs wegen gebietet, hängt von der Art, der Nähe und dem Ausmaß möglicher Gefahren, der Art und dem Rang des verfassungsrechtlich geschützten Rechtsguts sowie von den schon vorhandenen Regelungen ab.“[1320]

Die Gefahrenschwelle wird dabei teilweise in der Literatur an den polizei- und ordnungsrechtlichen Gefahrenbegriff angelehnt.[1321] Andere Stimmen in der Literatur lehnen eine derartige Übertragung polizeirechtlicher Maßstäbe ab und verlagern die Frage nach dem Umgang mit Belästigungen, sozialadäquaten Gefahrenlagen und Restrisiken in die Prüfung von Inhalt und Umfang der Schutzpflicht.[1322] Letztlich werden in der Sache aber dieselben Kriterien bemüht, so dass sich die Positionen anzunähern scheinen.[1323] Zentral ist jeweils die Relativität des Gefahrenbegriffs:[1324]

1319 Ausführlich dazu *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 227 ff.

1320 BVerfGE 49, 89, 142.

1321 Ausführlich dazu *Nitz*, Private und öffentliche Sicherheit, S. 381 ff.; *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 236, weitere Nachweise dazu siehe bei *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 76 f.

1322 *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 77 f. m.w.N.; *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 106; *Cremer*, Freiheitsgrundrechte, S. 286 ff.

1323 Besonders deutlich etwa bei *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 236 ff., der zunächst eine Übertragung des polizeirechtlichen Gefahrenbegriffs bejaht, sodann aber gerade den Ausschluss von Restrisiken aus dem Gefahrenbegriff ablehnt und diese vielmehr bei Inhalt und Umfang von Schutzpflichten geprüft sehen will. In der Sache bleibt damit kein Unterschied mehr zur Position etwa von *Isensee*, in: *Isensee/ Kirchhof,* HStR V, § 111, Rn. 106 ff., der den Rückgriff auf den polizeirechtlichen Gefahrenbegriff ablehnt, weil damit das „Risiko“ zu früh ausgeklammert werde, die Schutzpflicht erfasst seiner Auffassung nach grundsätzlich auch das Risiko, eine Abwägungsentscheidung dürfe erst auf Rechtsfolgenebene fallen.

1324 Vgl. etwa die Kriterien bei *Isensee*, Das Grundrecht auf Sicherheit, S. 37 f. Auch das BVerfG greift auf die Relativität des Gefahrenbegriffs zurück, s.o. BVerfGE 49, 89, 142: „…hängt von der Art, der Nähe und dem Ausmaß möglicher Gefahren […] ab.“

„Danach bestimmt sich die rechtlich erhebliche Gefahr nach dem Produkt aus Eintrittswahrscheinlichkeit und Schadensausmaß bzw. – umfang, so daß die erforderliche Wahrscheinlichkeit des Schadenseintritts mit steigendem Ausmaß des Schadens und der Bedeutung des bedrohten Rechtsguts abnimmt."[1325]

Unter Zugrundelegung dieser Maßstäbe liegt eine Gefahr von Rechtsgutsverletzungen vor:

- Ausmaß und Umfang potentieller Schäden sind gewaltig. Kommunikationsinhalte aller Art können betroffen sein. Streng vertrauliche Betriebs- und Geschäftsgeheimnisse können ebenso ausgeforscht werden wie eine aus Sicht der Betroffenen völlig belanglose E-Mail. Die besondere Bedeutung bestimmter Daten für den Grundrechtsträger kann zugleich eine gesteigerte Wichtigkeit des geschützten Rechtsguts bedeuten, muss dies aber nicht: Betriebs- und Geschäftsgeheimnisse etwa sind als eigentumsrechtliche Rechtsposition geschützt, unabhängig davon, ob es sich um ein Geheimnis der untersten Sicherheitsstufe handelt oder um höchst brisante Informationen: Der rechtliche Schutz des Rechtsguts bleibt gleich, die wirtschaftliche Bedeutung für den Grundrechtsträger ist exponentiell angestiegen. Bei privaten Geheimnissen würde dagegen ein Kernbereichsbezug nicht nur zu einer gesteigerten Wichtigkeit des Schutzes dieser Daten für den Betroffenen führen, sondern auch ein rechtlich besonders geschütztes Rechtsgut, die Menschenwürde, berühren. Besondere Schutzbedürftigkeit aus Sicht des Grundrechtsträgers und besonderer rechtlicher Schutz entsprechen sich in diesem Fall. Da es im vorliegenden Szenario um Daten geht, die sich in Händen des Staates befinden, dürfte eine Vermutung dafür sprechen, dass es sich um auch für außenstehende Dritte interessante Informationen handelt. Möglicherweise betroffen sein könnten: Steuerdaten, Daten aus elektronisch geführten Registern (vom Verkehrszentralregister bis zum Bundeszentralregister), Daten aus gerichtlichen Verfahren oder Verwaltungsverfahren (von der Beantragung einer Baugenehmigung bis zum Strafverfahren) etc.
- Dabei besteht eine hohe Eintrittswahrscheinlichkeit: Schäden können jederzeit eintreten. Hinsichtlich sämtlicher Datenkommunikation in öffentlichen Netzen, insbesondere im Internet, besteht ein enormes Überwachungs- und Abhörpotential. Jede Datenkommunikation – soweit sie eben nicht durch entsprechende IT-Sicherheitsmaßnahmen geschützt ist – kann überwacht, abgefangen und verändert werden. *Jede Datenkommunikation ist grundsätzlich immer gefährdet*. Ein Schadenseintritt ist jederzeit möglich.[1326]

Die Gefahrenschwelle ist somit überschritten; es besteht die Gefahr der Verletzung des geschützten Rechtsguts, der Vertraulichkeit individueller Telekommunikation. Es liegt gerade kein Fall eines *Risikos* (zum rechtlichen Risikobegriff s.o. in Teil 1 unter C.IV.3.b.) vor, da hinsichtlich der Informations- und Kommunikationstechnologie (jedenfalls für die hier relevanten Aspekte) keine kognitive tatsächliche

1325 *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 236 f.
1326 Daher dürfte sogar das Vorliegen einer unmittelbaren Gefahr anzunehmen sein.

Unsicherheit (mehr) herrscht: Die Gefahren von Überwachung und Abhören stehen objektiv fest.

b. Private als Störer

Die Rechtsgutsverletzung oder –gefährdung müsste von privaten Dritten als Störern ausgehen und nicht vom Staat oder dem Staat zurechenbaren Akteuren.

Vor allem unter Berufung auf die Mühlheim-Kärlich-Entscheidung des BVerfG[1327] wurde zum Teil eine staatliche Mitverantwortung als „Auslöser" von Schutzpflichten angesehen.[1328] Diese wurde aus einer der Genehmigungserteilung innewohnenden staatlichen „Verantwortungsübernahme" abgeleitet:

> „Wird aber ein Kernkraftwerk trotz des in ihm verkörperten außerordentlichen Gefährdungspotentials im Allgemeininteresse an der Energieversorgung genehmigt, so bedeutet dies, daß die körperliche Integrität Dritter Gefährdungen ausgesetzt werden kann, die diese nicht beeinflussen und denen sie kaum ausweichen können. Damit übernimmt der Staat seinerseits eine eigene Mitverantwortung für diese Gefährdungen. Demgemäß erscheint es geboten, bei der verfassungsrechtlichen Beurteilung der materiellrechtlichen und verfahrensrechtlichen Vorschriften für die Genehmigung von Kernkraftwerken nicht weniger strenge Maßstäbe anzulegen als bei der Prüfung staatlicher Eingriffsgesetze."[1329]

Diese Interpretation ist abzulehnen[1330] und hat auch in späteren Entscheidungen des BVerfG keinen Widerhall erfahren. Eine Zurechnung des Verhaltens des privaten Störers an den Staat kommt nicht in Betracht. Schutzpflichten werden dadurch weder begründet noch ausgelöst. Die Schutzpflichten ergeben sich einzig aus den jeweiligen Grundrechten. Jedes die geschützten Rechtsgüter beeinträchtigende private Verhalten – jenseits unerheblicher bloßer Belästigungen – aktiviert grundsätzlich die Schutzpflicht. Ob sich daraus konkrete Handlungsaufträge an den Staat ergeben, ist dann Frage von Inhalt und Umfang der Schutzpflicht und insbesondere der Güterabwägung.[1331]

Wesentlicher Unterschied zwischen abwehrrechtlicher und Schutzpflichtdimension ist gerade, ob die Rechtsbeeinträchtigung vom Staat oder von einem Privaten herrührt. Die Vermischung dieser beiden Kategorien im Wege einer staatlichen Mitverantwortung für privates Verhalten ist nicht weiterführend. Der Staat ist auch ohne

1327 BVerfGE 53, 30 – Mühlheim-Kärlich.

1328 *Isensee*, Das Grundrecht auf Sicherheit, S. 29.

1329 BVerfGE 53, 30, 58.

1330 So auch *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, S. 92 ff.

1331 Zum Teil wird in der Literatur aus staatlicher Mitverantwortung eine höhere Schutzintensität abgeleitet; vgl. etwa *Möstl,* DÖV 1998, 1029, 1036: „Einen dem Abwehrrecht nahekommenden Schutz vermag die Schutzpflicht zu vermitteln, wenn sich die vom Staat und von Privaten ausgehenden Gefahren für das Grundrecht nach Art und Intensität gleichen oder wenn für die private Gefahr eine besondere staatliche (Mit-)Verantwortung festgestellt werden kann." Auch *Möstl* verankert diesen Gedanken aber – wie auch hier vorgeschlagen – innerhalb der Güterabwägung.

eine solche Verantwortungsübernahme zum Schutz verpflichtet, sei es wegen des Menschenwürdeschutzauftrages, sei es als Staatsaufgabe.

Die Schutzpflichtdimension ist – wie bereits dargestellt – eine eigenständige Grundrechtsdimension und nicht lediglich eine Variante des abwehrrechtlichen Grundrechtsgehalts. Prägend für die grundrechtlichen Schutzpflichten ist die Dreieckskonstellation von Grundrechtsberechtigtem (häufig auch als Opfer bezeichnet), privatem Störer und Staat.[1332] Die Figur einer besonderen staatlichen Mitverantwortung vermag der Schutzpflichtendogmatik nichts Wesentliches hinzuzufügen, verwischt aber die klaren Grenzen zwischen abwehrrechtlicher Grundrechtsdimension und Schutzpflichtdimension.

4. Inhalt und Umfang der Schutzpflicht

Zentrale Frage ist, welchen Inhalt und welchen Umfang eine staatliche Schutzpflicht aus dem Fernmeldegeheimnis (Art. 10 I GG) hat, kurz gesagt: Was genau muss der Staat tun, um das Fernmeldegeheimnis zu schützen?

a. Gesetzesmediatisierung der Schutzpflicht

Die Erfüllung von Schutzpflichten erfordert in der Regel eine Rechtsgrundlage:[1333] Da der Schutz der Grundrechte des Opfers zumeist durch einen Eingriff in die Grundrechte des Störers bewirkt wird, ist regelmäßig eine gesetzliche Grundlage erforderlich.[1334] Außerdem sind Schutzpflichten so abstrakt, dass sie nach den Maßstäben der Wesentlichkeitstheorie von Seiten des Gesetzgebers konkretisierungsbedürftig sind.[1335] Es verbleiben nur wenige denkbare Konstellationen, in denen ohne einfachgesetzliche Grundlage staatliche Schutzpflichten erfüllt werden; ein Beispiel könnten etwa Warnungen der Bundesregierung zum Schutz vor akuten Gesundheitsgefahren sein.[1336]

1332 *Isensee*, Das Grundrecht auf Sicherheit, S. 34 ff.; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 21, vgl. zu der grundrechtlich fundierten Dreieckskonstellation *Wahl/Masing,* JZ 1990, 553, 556.

1333 Siehe ausführlich *Isensee*, Das Grundrecht auf Sicherheit, S. 42 ff.; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 23 f.

1334 *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 23; *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 149.

1335 *Isensee*, Das Grundrecht auf Sicherheit, S. 42; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 24; *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 152; *Nitz*, Private und öffentliche Sicherheit, S. 386.

1336 Hier wurde für Warnungen vor mit Glykol versetztem Wein eine Annexkompetenz der Bundesregierung zu Information der Bevölkerung angenommen; vgl. BVerfG, Beschluss vom 26.06.2002, Az.: 1 BvR 558/91 und 1428/91, Rn. 53 ff. Inhaltlich setzten die Warnungen vor

Jenseits derartiger besonderer Konstellationen, in denen sich aus dem Grundgesetz selbst eine Rechtsgrundlage für staatliches Handeln ergibt, erfordert die Schutzpflichterfüllung eine gesetzliche Grundlage, erfolgt also gesetzesmediatisiert. Dabei ist nicht unbedingt die Schaffung neuer Ermächtigungsgrundlagen erforderlich, insbesondere Generalklauseln erlauben häufig eine Berücksichtigung von Schutzpflichten bereits de lege lata.[1337] Im Übrigen ist der Gesetzgeber zum Erlass einer gesetzlichen Grundlage für die Schutzpflichterfüllung aufgerufen. Exekutive und Judikative sind an diese gesetzliche Norm ebenso wie an sonstige Rechtsnormen gebunden und müssen ihnen etwaig eingeräumtes Ermessen schutzpflichtkonform ausüben (bzw. im Fall der richterlichen Kontrolle die Restriktion der gerichtlichen Überprüfung auf Ermessensfehler beachten). Entscheidend bei der Frage nach der Art und Weise der Schutzpflichterfüllung ist daher die gesetzgeberische Gestaltung, zumal es sich regelmäßig auch um eine politische Entscheidung handeln dürfte. Daher wird im Folgenden vor allem auf die gesetzgeberische Entscheidung abgestellt, auch wenn dies nicht die einzige Art der Schutzpflichterfüllung darstellt; gleichwohl ist es die quantitativ wie qualitativ wichtigste.

b. Weiter Einschätzungs-, Wertungs- und Gestaltungsspielraum

Bei der Erfüllung von Schutzpflichten kommt dem Gesetzgeber grundsätzlich ein weiter Einschätzungs-, Wertungs- und Gestaltungsspielraum zu:[1338]

> „Dem Gesetzgeber wie der vollziehenden Gewalt kommt bei der Erfüllung dieser Schutzpflichten ein weiter Einschätzungs-, Wertungs- und Gestaltungsbereich zu, der auch Raum läßt, etwa konkurrierende öffentliche und private Interessen zu berücksichtigen. Diese weite Gestaltungsfreiheit kann von den Gerichten je nach Eigenart des in Rede stehenden Sachbereichs, den Möglichkeiten, sich ein hinreichend sicheres Urteil zu bilden und der Bedeutung der auf dem Spiele stehenden Rechtsgüter nur in begrenztem Umfang überprüft werden.“[1339]

Dies ist überzeugend: Würde man dem BVerfG, oder allgemeiner der Judikative, hier eine stärkere Kontrolle zugestehen, würde dies unweigerlich zu einer Machtverschiebung innerhalb des Gewaltenteilungskonzepts des Grundgesetzes führen – was insbesondere auch gegen die Annahme objektiv-rechtlicher Grundrechtsgehalte eingewandt wurde:[1340]

gesundheitsschädlichen Zusätzen im Wein die staatliche Schutzpflicht aus Art. 2 II S. 1 GG um.

1337 *Isensee*, Das Grundrecht auf Sicherheit, S. 43; *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 154.

1338 *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 162; *Isensee*, Das Grundrecht auf Sicherheit, S. 39 ff.; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 80 ff.; *Möstl,* DÖV 1998, 1029, 1037; *Dreier*, in: *Dreier,* GG, Vorbemerkung, Rn. 103.

1339 BVerfGE 77, 170, 214 f.

1340 *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 54; *Böckenförde,* Der Staat 1990, 1, 24 f; ausführlich dazu auch *Cremer*, Freiheitsgrundrechte, S. 298 ff.

„Es vollzieht sich ein gleitender Übergang vom parlamentarischen Gesetzgebungsstaat zum verfassungsrechtlichen Jurisdiktionsstaat. Er vollzieht sich auf dem Weg über die Entfaltung der Grundrechte als objektive Grundsatznormen und die Kompetenz des Verfassungsgerichts zu deren Konkretisierung. Die Aufgabe des BVerfG verändert sich insoweit von rechtsanwendender Rechtsprechung zu verfassungsbezogener Jurisdictio im alten Sinn, die der Trennung von Rechtsetzung und Rechtsanwendung vorausliegt."[1341]

Letztlich wäre dann nicht mehr die Einschätzung oder Bewertung des parlamentarischen Gesetzgebers entscheidend, sondern deren Billigung oder Missbilligung durch das BVerfG.

„Diese Begrenzung der verfassungsrechtlichen Nachprüfung erscheint deshalb geboten, weil es regelmäßig eine höchst komplexe Frage ist, w i e eine positive staatliche Schutz- und Handlungspflicht, die erst im Wege der Verfassungsinterpretation aus den in den Grundrechten verkörperten Grundentscheidungen hergeleitet wird, durch aktive gesetzgeberische Maßnahmen zu verwirklichen ist. Je nach der Beurteilung der tatsächlichen Verhältnisse, der konkreten Zielsetzungen und ihrer Priorität sowie der Eignung der denkbaren Mittel und Wege sind verschiedene Lösungen möglich. Die Entscheidung, die häufig Kompromisse erfordert, gehört nach dem Grundsatz der Gewaltenteilung und dem demokratischen Prinzip in die Verantwortung des vom Volk unmittelbar legitimierten Gesetzgebers und kann vom Bundesverfassungsgericht in der Regel nur begrenzt nachgeprüft werden, sofern nicht Rechtsgüter von höchster Bedeutung auf dem Spiele stehen."[1342]

Schließlich hat *Alexy* überzeugend ausgeführt, dass sich ein Spielraum bei der Erfüllung von Schutzpflichten unmittelbar aus deren Wesen ergibt:[1343]

„Wenn es *verboten* ist, etwas zu zerstören oder zu beeinträchtigen, dann ist *jede* Handlung, die eine Zerstörung oder Beeinträchtigung darstellt oder bewirkt, verboten. Demgegenüber ist dann, wenn es *geboten* ist, etwas zu schützen oder zu fördern, *nicht jede* Handlung, die einen Schutz oder eine Förderung darstellt oder bewirkt, geboten. So impliziert das Tötungsverbot jedenfalls prima facie das Verbot jeder Tötungshandlung, das Rettungsgebot demgegenüber nicht das Gebot jeder Rettungshandlung. Wenn es möglich ist, einen Ertrinkenden sowohl schwimmend als auch durch den Wurf eines Rettungsringes als auch mit Hilfe eines Bootes zu retten, sind keinesfalls alle drei Rettungshandlungen zugleich geboten. Geboten ist vielmehr, die erste *oder* die zweite *oder* die dritte Handlung vorzunehmen. Dies heißt aber, daß der Adressat des Rettungsgebotes, wenn nicht weitere Gründe einschränkend hinzutreten, einen *Spielraum* hat, innerhalb dessen er wählen kann, wie er das Gebot erfüllen will."[1344]

c. Grenze: Untermaßverbot

Dieser weite gesetzgeberische Spielraum bei der Erfüllung von Schutzpflichten findet seine Grenze aber im Untermaßverbot.[1345]

1341 *Böckenförde,* Der Staat 1990, 1, 25.
1342 BVerfGE 56, 54, 81.
1343 So auch *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 26.
1344 *Alexy*, Theorie der Grundrechte, S. 420 f.
1345 *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 165; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 80 ff. mit ausführlicher Darstelllung der Entwicklung der Recht-

„Art und Umfang des Schutzes im einzelnen zu bestimmen, ist Aufgabe des Gesetzgebers. Die Verfassung gibt den Schutz als Ziel vor, nicht aber seine Ausgestaltung im einzelnen. Allerdings hat der Gesetzgeber das *Untermaßverbot* zu beachten; insofern unterliegt er der verfassungsgerichtlichen Kontrolle."[1346]

Das Untermaßverbot im Rahmen der Schutzpflichtdimension entspricht dem Übermaßverbot in der abwehrrechtlichen Dimension,[1347] sprich: dem Verhältnismäßigkeitsgrundsatz.[1348] Über- und Untermaßverbot sind dabei aber weder dogmatisch[1349] noch inhaltlich[1350] identisch. Beides sind besondere Ausprägungen des allgemeinen Verhältnismäßigkeitsgrundsatzes, unterscheiden sich aber in zentralen Punkten. Geht es beim abwehrrechtlichen Übermaßverbot allein um den Ausgleich zwischen verfolgtem Zweck und beeinträchtigtem Rechtsgut, *spielt bei der Schutzpflichterfüllung der Verhältnismäßigkeitsgrundsatz zweifach eine Rolle: Zum einen in der Form des Untermaßverbots als untere Grenze dessen, was als verhältnismäßige Schutzpflichterfüllung des Staates gelten kann. Zum anderen aber gleichzeitig in Form des Übermaßverbots als obere Grenze der zulässigen Eingriffe in die Grundrechtsposition des Störers*.[1351]

„Beim ambivalenten Schutzeingriff gegen den Störer, der dessen Abwehrrecht zu wahren und das Schutzbedürfnis des Opfers zu erfüllen hat, sind die gegenläufigen Maximen zum Ausgleich zu bringen. Der Rechtsstaat steht hier von zwei Seiten unter grundrechtlichem Rechtfertigungszwang: vom Störer, wenn er in sein Grundrecht eingreift, oder vom Schutzbedürftigen, wenn er ihm den Schutz vorenthält."[1352]

Zwischen der unteren Schwelle des Untermaßverbots sowie der Obergrenze des Übermaßverbots liegt der gesetzgeberische Einschätzungs-, Wertungs- und Gestaltungsspielraum:[1353]

sprechung des BVerfG; *Möstl,* DÖV 1998, 1029, 1038 sowie ausführlich und mit weiteren Nachweisen *Cremer*, Freiheitsgrundrechte, S. 310 ff.

1346 BVerfGE 88, 203, 254.

1347 *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 165; *Dreier*, in: *Dreier,* GG, Vorbemerkung, Rn. 103.

1348 *Dreier*, in: *Dreier,* GG, Vorbemerkung, Rn. 145; *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 30; *Cremer*, Freiheitsgrundrechte, S. 311.

1349 *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 30.

1350 Nach der so genannten Kongruenzthese wird teilweise in der Literatur vertreten, Über- und Untermaßverbot seien im Ergebnis identisch; siehe im Einzelnen dazu *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 85 ff. sowie *Nitz*, Private und öffentliche Sicherheit, S. 373 ff. und *Cremer*, Freiheitsgrundrechte, S. 312 ff. Auch diese Auffassung verneint aber nicht grundsätzlich einen gesetzgeberischen Spielraum, verankert diesen nur nicht zwischen Untermaßverbot als Untergrenze und Übermaßverbot als oberer Grenze, sondern im Rahmen des Verhältnismäßigkeitsgrundsatzes an sich (*Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 86). Dem Untermaßverbot komme daneben keine eigenständige Bedeutung zu.

1351 *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 84; *Möstl,* DÖV 1998, 1029, 1038.

1352 *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 165.

1353 *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 33; *Nitz*, Private und öffentliche Sicherheit, S. 371 f.

„Der Gesetzgeber *muß* zumindest soweit in das Grundrecht des Dritten eingreifen, als dies die dem geförderten Grundrecht entfließende Schutzpflicht gebietet. Darüber hinaus muß er nicht gehen, *kann* es aber, bis hin zur praktischen Konkordanz der beiden Grundrechte."[1354]

Dies ist neben den inhaltlichen Besonderheiten der Schutzpflicht bei der *Prüfung des Untermaßverbots* zu beachten.[1355]

- Dabei ist zunächst zu prüfen, ob überhaupt ein *staatliches Schutzkonzept* im Hinblick auf die Rechtsgutsbeeinträchtigungen besteht.[1356]
- Danach ist zu prüfen, ob dieses staatliche Schutzkonzept *geeignet* ist, das Rechtsgut zu schützen.
- Dann ist die Frage zu beantworten, ob es ein ebenso mildes, aber *effektiveres* Schutzkonzept gibt.
- Zuletzt ist zu prüfen, ob der Schutz unter Berücksichtigung entgegenstehender Rechtsgüter *angemessen* ist.[1357]

Klar ist, dass das Kriterium der Effektivität[1358] des Rechtsgüterschutzes Berücksichtigung finden muss – auch nach der Rechtsprechung des BVerfG:[1359]

1354 *Jarass,* AöR 1985, 363, 384.

1355 Prüfungsstruktur im Wesentlichen nach *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 31 ff. und *Möstl*, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, S. 1038 f. Ähnlich auch *Nitz*, Private und öffentliche Sicherheit, S. 375 f. Einen abweichenden Vorschlag macht dagegen *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 253 f. Dieser prüft nicht die Verhältnismäßigkeit eines staatlichen Schutzkonzepts, sondern fragt umgekehrt danach, ob bestimmte Rechtspositionen die Unterlassung von Schutzmaßnahmen rechtfertigen können. Damit rückt aber die Entfaltung dieser anderen Rechtspositionen in den Mittelpunkt der Prüfung und nicht mehr die Frage, wie optimalerweise die Schutzpflichten umzusetzen wären. Erst nach einer Konkretisierung, welche Maßnahmen allein aus der Schutzpflichtperspektive zu treffen wären, können diese Schutzpflichtbelange sinnvoll mit entgegenstehenden Belangen abgewogen werden. Der Ansatz von *Hermes* berücksichtigt so nicht ausreichend das bipolare Spannungsverhältnis der verschiedenen widerstreitenden Grundrechtspositionen, sondern denkt auch die Verhältnismäßigkeitsprüfung nach wie vor aus der abwehrrechtlichen Perspektive. Erforderlich ist aber die Kombination von abwehrrechtlicher und Schutzpflichtperspektive.

1356 Existiert – wie zumeist – ein staatliches Schutzkonzept, ist dies sodann der weiteren Prüfung zu unterziehen. Existiert dagegen kein staatliches Schutzkonzept (echtes staatliches Unterlassen), könnte höchstens fiktiv bezüglich einzelner denkbarer Schutzmaßnahmen deren Verfassungsmäßigkeit geprüft werden. Unter mehreren zulässigen Schutzkonzepten bleibt die Wahl aber dem Gesetzgeber vorbehalten. Konstellationen, in denen sich nur eine verfassungsgemäße Option bietet, sind äußerst selten. Ausführlich dazu sowie zur Frage, welche denkbaren Schutzmaßnahmen vom BVerfG verfassungsrechtlich zu prüfen sind *Cremer*, Freiheitsgrundrechte, S. 272 ff.

1357 Die Bezeichnung Angemessenheit wurde gewählt, da es sich bei der im Rahmen der Schutzpflichten zu treffenden Abwägungsentscheidung gerade nicht um die Verhältnismäßigkeit im engeren Sinne des Übermaßverbots handelt, sondern vielmehr um eine „Angemessenheits-Verhältnismäßigkeit": „Bei ihr geht es darum, Vereinbarkeit, Ausgleich, angemessenen Zuordnung mehrerer, auch gegenläufiger normativer Prinzipien zu erreichen."; *Böckenförde,* Der Staat 1990, 1, 20; in der Sache dürfte *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 33 dasselbe meinen.

„Wie die staatlichen Organe ihre Verpflichtung zu einem effektiven Schutz des Lebens erfüllen, ist von ihnen grundsätzlich in eigener Verantwortung zu entscheiden. Sie befinden darüber, welche Schutzmaßnahmen zweckdienlich und geboten sind, um einen wirksamen Lebensschutz zu gewährleisten. Ihre Freiheit in der Wahl der Mittel zum Schutz des Lebens kann sich in besonders gelagerten Fällen auch auf die Wahl eines bestimmten Mittels verengen, wenn ein effektiver Lebensschutz auf andere Weise nicht zu erreichen ist.“[1360]

Zumeist wird das Erforderlichkeitskriterium des Übermaßverbots bei der Prüfung des Untermaßverbots durch das Effektivitätskriterium ersetzt,[1361] da die Entscheidung, welche Maßnahmen als erforderlich angesehen werden, im Ermessen des Gesetzgebers liegt. Die Erforderlichkeit unterliegt angesichts des gesetzgeberischen Einschätzungs-, Wertungs- und Gestaltungsspielraums gerade nicht der gerichtlichen Überprüfung. Die Frage, ob der so bewirkte Rechtsgüterschutz effektiv ist, wird dagegen gerichtlich überprüft, so dass das Erforderlichkeits- durch das Effektivitätskriterium zu ersetzen ist.

aa) Staatliches Schutzkonzept?

Im ersten Schritt ist zu ermitteln, ob es ein staatliches Schutzkonzept gibt und aus welchen Maßnahmen es besteht. Zur Umsetzung der Schutzpflicht aus dem Fernmeldegeheimnis (Art. 10 I GG) existiert ein staatliches Schutzkonzept, wie schon der Blick auf den einfachgesetzlichen Schutz des Fernmeldegeheimnisses in § 88 TKG, die gesetzliche Verpflichtung zum technischen Schutz des Fernmeldegeheimnisses durch die Diensteanbieter nach § 109 I Nr. 1 TKG sowie den strafrechtlichen Schutz des Fernmeldegeheimnis in § 206 StGB zeigt. Daneben können zahlreiche weitere Normen genannt werden, die zumindest auch dem Schutz des Fernmeldegeheimnisses dienen, aus dem strafrechtlichen Bereich etwa § 202a StGB, der das unbefugte Ausspähen von Daten,[1362] sowie § 202b StGB, der das Abfangen von Daten aus nichtöffentlichen Datenübermittlungen unter Strafe stellt.

Da es hier aber allein um den Einsatz von Verschlüsselungstechnologien geht, beschränkt sich die Darstellung des Schutzkonzepts auf staatliche Maßnahmen, die mit

1358 Dieser Forderung liegt aber nicht das bei *Nitz*, Private und öffentliche Sicherheit, S. 376 formulierte Optimierungsgebot zu Grunde, demzufolge ein staatlicher Grundrechtseingriff wenigstens effektiv sein müsse, wenn er denn schon stattfinde.

1359 Dies wurde zum Teil für überflüssig gehalten; *Nitz*, Private und öffentliche Sicherheit, S. 376. Die Forderung größtmöglicher Effektivität der Schutzmaßnahmen basiere auf der – nach dieser Auffassung – falschen Vorstellung, bei den Schutzpflichten handele es sich um Optimierungsgebote. Allerdings fordert *Nitz* die Einhaltung eines „Mindestschutzniveaus“ (ebenda, S. 379), dem ebenfalls der Effektivitätsgedanke inhärent ist.

1360 BVerfGE 46, 160, 164 f.

1361 *Nitz*, Private und öffentliche Sicherheit, S. 375 prüft dagegen im Rahmen der Geeignetheit die „Geeignetheit zu *wirksamem* Schutz“, was im Kern eigentlich nicht die Fragestellung bei der Geeignetheit darstellt.

1362 Auch bei deren Übermittlung, wie sich aus § 202a II StGB ergibt.

dem Einsatz von Verschlüsselung bei der Datenübertragung via Telekommunikation in Zusammenhang stehen (können):[1363]

- Bei Datenübermittlungen bestehen einige einfachgesetzliche *explizite Verschlüsselungspflichten* (s.o. in Teil 1 unter C.II.1.)
- Viele einfachgesetzliche Normen fordern den Schutz der *„Vertraulichkeit"*, den *Schutz „gegen unbefugte Kenntnisnahme"* u.ä. Wegen der besonderen Kenntnisnahmegefahren ergeben sich daraus für Datenübermittlungen in allgemein zugänglichen Netzen (wie dem Internet) in teleologischer Auslegung *implizite Verschlüsselungspflichten* (s.o. in Teil 1 unter C.II.2.a.). Sind besonders schutzwürdige Daten (sensible Daten oder Daten mit einem besonders hohen Verknüpfungspotential) betroffen, dann ergeben sich auch bei Datenübermittlungen in lokalen Netzen (Intranets etwa) implizite Verschlüsselungspflichten (s.o. in Teil 1 unter C.II.2.b.).

1363 Dabei kann es sich – soweit es um den Schutzbereich des Fernmeldegeheimnisses geht – nur um solche Regelungen handeln, die entweder Kommunikation zwischen Grundrechtsberechtigten und Staat oder von Grundrechtsberechtigten untereinander zum Gegenstand haben. Geht es um Datenübermittlungen zwischen Behörden (was den Großteil der Regelungen zu Vertraulichkeit bei Informationsübermittlung via Telekommunikationstechnik ausmacht) dienen Vertraulichkeitsanforderungen allein dem Schutz des allgemeinen Persönlichkeitsrechts, insbesondere in Form des Rechts auf informationelle Selbstbestimmung (Art. 2 I GG i.V.m. Art. 1 I GG). In der Sache geht es um die allgemeine Frage, wie staatliche Stellen mit Daten des Einzelnen umzugehen haben, welche Sorgfaltspflichten sie dabei treffen usw. Das ist klar eine Fragestellung des allgemeinen Persönlichkeitsrechts, insbesondere des Rechts auf informationelle Selbstbestimmung sowie des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Die Vertraulichkeitsgefährdung bei der Informationsübermittlung von einer staatlichen Stelle an eine andere staatliche Stelle beruht im Wesentlichen nicht darauf, dass wegen der Notwendigkeit des Einsatzes eines Übermittlers eine besondere Zugriffsmöglichkeit – insbesondere staatlicher Stellen (!) – bestünde. Die Gefährdung für die Daten des Einzelnen beruht vor allem auf möglicherweise rechtswidriger Weitergabe, Speicherung und Aufbewahrung von Daten. Die Gefahr der Kenntnisnahme durch andere staatliche Stellen im Wege von Abhörmaßnahmen dürfte dagegen gerade nicht bestehen. Sicherlich kommt bei einer Datenübermittlung via Internet die Gefahr der Ausspähung der Daten durch private Dritte hinzu. Schwerpunktmäßig geht es aber um Fragen des staatlichen Umgangs mit (personenbezogenen) Daten, und somit um informationelle Selbstbestimmung und Datenschutz. Für diese Betrachtungsweise spricht, dass das Fernmeldegeheimnis in einer abwehrrechtlichen Perspektive bei der Weitergabe von Daten an andere staatliche Stellen nur dann betroffen ist, wenn bereits die Erhebung der Daten einen Eingriff in das Fernmeldegeheimnis dargestellt hatte oder dargestellt hätte (vgl. dazu ausführlicher *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 51). In einer Schutzpflichtenperspektive kann nichts anderes gelten, zumal die Übereinstimmung der Schutzbereiche in abwehrrechtlicher wie Schutzpflichtdimension bereits herausgearbeitet wurde (s.o. unter I.2.c.). Auch wenn Datenübermittlungen von Behörde zu Behörde damit im Einzelfall (vor allem im Bereich des Strafrechts) auch Daten enthalten können, die unter Verstoß gegen das Fernmeldegeheimnis erhoben wurden und deren Weitergabe somit ebenfalls einen Verstoß gegen das Fernmeldegeheimnis darstellt, konzentriert sich diese Darstellung des staatlichen Schutzkonzepts auf Normen, die vornehmlich dem Schutz des Fernmeldegeheimnisses dienen und nicht nur bei Gelegenheit.

Als besonders schutzwürdig in diesem Sinne sind in einer grundrechtskonformen Auslegung auch sämtliche in den Schutzbereich des Fernmeldegeheimnisses (Art. 10 I GG) fallenden Daten anzusehen:

„Die Schutzverpflichtung des Staates muß umso ernster genommen werden, je höher der Rang des in Frage stehenden Rechtsgutes innerhalb der Wertordnung des Grundgesetzes anzusetzen ist.“[1364]

Die durch das Fernmeldegeheimnis geschützten Daten unterliegen einem besonderen grundrechtlichen Schutz. Es handelt sich sowohl um eine spezielle Privatsphärengewährleistung mit Bezug zur Menschenwürde als auch um ein in einem demokratischen Rechtsstaat elementares Kommunikationsgrundrecht. Daraus folgt, dass wegen der besonderen Vertraulichkeitsgefahren bei einer Datenübermittlung durch Telekommunikationstechnik und dem besonderen Vertraulichkeitsschutz, den das Grundgesetz für Telekommunikationsdaten gewährt, im Wege der verfassungskonformen Auslegung stets eine *implizite Verschlüsselungspflicht für Telekommunikationsdaten* zum Schutz der „Vertraulichkeit“, zum Schutz „gegen unbefugte Kenntnisnahme“ etc. anzunehmen ist.

- Auch aus dem Erfordernis *technisch-organisatorischer Datenschutzmaßnahmen* bei Datenübermittlungen aus Satz 2, Nr. 4 der Anlage zu § 9 S. 1 BDSG und – in Hessen – § 10 II Satz 2, Nr. 4 HDSG ergeben sich *Verschlüsselungspflichten* (s.o. in Teil 1 unter C.II.7.a.). Auch hier ergibt sich bei Datenübermittlungen in allgemein zugänglichen Netzen eine Verschlüsselungspflicht. Dementsprechend nennt Satz 3 der Anlage zu § 9 S. 1 BDSG seit 01.09.2009 auch ausdrücklich und insbesondere Verschlüsselung als technische-organisatorische Maßnahme der Weitergabekontrolle (Satz 2, Nr. 4 der Anlage zu § 9 S. 1 BDSG).[1365] Zwar sind nach § 9 S. 2 BDSG und § 10 I S. 2 HDSG nur solche technischen und organisatorischen Maßnahmen erforderlich, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Aufgrund der Bedeutung des Fernmeldegeheimnisses (sowohl hinsichtlich des Schutzes der Privatsphäre als auch als elementares Kommunikationsgrundrecht in einem demokratischen Rechtsstaat) ist der Einsatz von Verschlüsselung in allgemein zugänglichen Netzen aber *stets* als *angemessen* in diesem Sinne anzusehen.

Zusammenfassend kann festgehalten werden: Vereinzelt bestehen hinsichtlich besonders schutzwürdiger Daten (etwa Melde-, Steuer- oder Sozialdaten) explizite gesetzliche Verschlüsselungspflichten bei Datenübermittlungen. Für den Großteil der Datenübermittlungen ergibt sich nur implizit eine Verschlüsselungspflicht, entweder in verfassungskonformer Auslegung von einfachgesetzlichen Normen, die den Schutz der „Vertraulichkeit“, den Schutz „gegen unbefugte Kenntnisnahme“ oder ähnliches vorschreiben, oder in verfassungskonformer Auslegung der bei Datenübermittlungen zu treffenden technisch-organisatorischen Datenschutzmaßnahmen.

1364 BVerfGE 39, 1 42.

1365 Satz 3 der Anlage zu § 9 S. 1 BDSG in der Fassung vom 14.08.2009 (BGBl. I, 2814): “Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.“

Im Anwendungsbereich des BDSG wird Verschlüsselung insbesondere als technisch-organisatorische Maßnahme bei Datenübermittlungen genannt, daraus ergibt sich in verfassungskonformer Auslegung ebenfalls eine *Pflicht* zur Verschlüsselung.

bb) Geeignetheit

Zu prüfen ist, ob dieses staatliche Schutzkonzept geeignet ist, das Rechtsgut, hier die Vertraulichkeit der räumlich distanzierten Individualkommunikation, zu schützen. Erforderlich ist insoweit nur, dass der Schutz des Rechtsgutes durch das staatliche Schutzkonzept gefördert wird. Die dargestellten einfachgesetzlichen Regelungen, die einen Vertraulichkeitsschutz insbesondere bei Übermittlung der geschützten Daten vorsehen, fördern zweifelsohne den Schutz des Fernmeldegeheimnisses. Die Eignung der staatlichen Maßnahmen zum Schutz des Fernmeldegeheimnisses liegt daher vor; ob dieser Schutz ausreichend ist, ist keine Frage der Geeignetheit.

cc) Effektivität

Des Weiteren müsste das staatliche Schutzkonzept effektiv sein.[1366]

(1) Prüfungsmaßstab

Verlangt wird dabei aber *nicht das effektivste aller denkbaren Schutzkonzepte*: Absoluten Schutz und absolute Sicherheit kann es nicht geben.[1367] Außerdem sind Freiheits- und Sicherheitsinteressen in einer verfassungsrechtlichen Perspektive in einen angemessenen *Ausgleich* zu bringen. Die hundertprozentige Verfolgung des Interesses „Sicherheit“ zu Lasten des Interesses „Freiheit“ kann angesichts der widerstreitenden Interessen Freiheit – Sicherheit[1368] nicht verfassungskonform sein.

1366 Siehe zu grundlegenden Fragen der Feststellbarkeit der Effektivität von Recht *Holtschneider*, Normenflut und Rechtsversagen, S. 127 ff.

1367 *Isensee*, Das Grundrecht auf Sicherheit, S. 41.

1368 Natürlich kann man auch umgekehrt argumentieren, dass wirkliche Freiheit ohne Sicherheit nicht denkbar ist und dass auch die Sicherheit gefährdet ist, wenn es keine Freiheit gibt. Zunächst sollen Sicherheit und Freiheit aber als widerstreitende Interessen begriffen werden, da in der Regel ein Mehr an Sicherheit ein Weniger an Freiheit bedeutet und ein Mehr an Freiheit häufig ein Weniger an Sicherheit nach sich ziehen dürfte. Dass sich dabei Sicherheit und Freiheit auch gegenseitig bedingen, verschärft nur die Komplexität der zu treffenden Abwägungsentscheidung zwischen diesen Belangen, ändert aber nichts an der grundsätzlichen Einstufung als gegenläufige Prinzipien.

Daher ist vielmehr zu fragen, ob es *bei gleich mildem Eingriff* in entgegenstehende Rechtsgüter ein *effektiveres Schutzkonzept* zu Gunsten der geschützten Rechtsgüter gibt.[1369] Dabei sind zwei Fragen zu unterscheiden:

- Zunächst ist zu prüfen, ob das staatliche Schutzkonzept *überhaupt effektiv* ist.
- Dann ist die Frage zu beantworten, ob es ein *ebenso mildes, aber effektiveres* Schutzkonzept gibt. Diese Fragestellung führt – entgegen teilweise geäußerter Befürchtungen[1370] – nicht dazu, dass Schutzpflicht und Abwehrrecht quasi nur im Wege *eines* punktgenauen Schutzniveaus miteinander in Einklang gebracht werden können. Die Gewichtung der Interessen, ein Mehr oder Weniger an Schutz oder Eingriff sind genau die zentralen Wertungsfragen, die allein – bis zur Grenze der Unvertretbarkeit[1371] – dem Gesetzgeber vorbehalten sind. Gutes Beispiel ist etwa der Nichtraucherschutz: Hier hat es das BVerfG[1372] für verfassungsrechtlich zulässig gehalten, ein striktes Rauchverbot in Gaststätten zu verhängen und so der Schutzpflicht für die Gesundheit aus Art. 2 II S. 1 GG eindeutig den Vorrang vor der Berufsfreiheit und der allgemeinen Handlungsfreiheit einzuräumen.[1373] Andererseits kann sich der Gesetzgeber nach der Rechtsprechung des BVerfG auch dafür entscheiden, Ausnahmetatbestände vom Rauchverbot zuzulassen und so auch die Interessen der Gaststättenbetreiber sowie der Raucher zu berücksichtigen.[1374]

1369 Hier zeigt sich erneut der Zusammenhang der Erforderlichkeit im Übermaßverbot und der Effektivität beim Untermaßverbot: Es geht jeweils um möglichst hohe Schutzintensität bei möglichst geringer Rechtsgutsbeeinträchtigung.

1370 *Nitz*, Private und öffentliche Sicherheit, S. 371.

1371 Teilweise sprach sich das BVerfG neben der „Vertretbarkeitskontrolle“ aber auch für eine „Evidenzkontrolle“ bis hin zu einer „intensivierten inhaltlichen Kontrolle“ aus – je nach Sachbereich, Prognosemöglichkeiten und betroffenen Rechtsgütern; BVerfGE 50, 290, 232 f. Später hat das BVerfG dann unter ausdrücklicher Bezugnahme auf das soeben genannte Urteil entschieden, dass in jedem Fall eine Vertretbarkeitskontrolle stattfinde: „Ob sich hieraus für die verfassungsrechtliche Überprüfung drei voneinander unterscheidbare Kontrollmaßstäbe herleiten lassen bedarf keiner Erörterung; die verfassungsrechtliche Prüfung erstreckt sich in jedem Falle darauf, ob der Gesetzgeber die genannten Faktoren ausreichend berücksichtigt und seinen Einschätzungsspielraum "in vertretbarer Weise" gehandhabt hat.“; BVerfGE 88, 203, 262. Siehe dazu ausführlich *Cremer*, Freiheitsgrundrechte, S. 291 ff., der auch nachweist, dass in der jüngeren Rechtsprechung des BVerfG häufig auch nur noch eine Evidenzkontrolle staatfindet, d.h., dass nur eine eindeutige Überschreitung der Ermessensgrenze durch den Gesetzgeber (so BVerfGE 36, 1, 17) vom BVerfG geprüft wird.

1372 BVerfG, Urteil vom 30.07.2008, Az.: 1 BvR 3262/07 et al.

1373 BVerfG, Urteil vom 30.07.2008, Az.: 1 BvR 3262/07 et al., Rn. 121: „Auf der Grundlage der ihm zuzubilligenden Spielräume wäre der Gesetzgeber nicht gehindert, dem Gesundheitsschutz gegenüber den damit beeinträchtigten Freiheitsrechten, insbesondere der Berufsfreiheit der Gastwirte und der Verhaltensfreiheit der Raucher, den Vorrang einzuräumen und ein striktes Rauchverbot in Gaststätten zu verhängen.“

1374 BVerfG, Urteil vom 30.07.2008, Az.: 1 BvR 3262/07 et al., Rn. 129: „Zwar hätte der Gesetzgeber, wie ausgeführt, die gegenläufigen Interessen der Gaststättenbetreiber und der Raucher im Ergebnis auch vollständig zurücktreten lassen dürfen. Dies hindert ihn angesichts des ihm zukommenden Einschätzungs-, Wertungs- und Gestaltungsspielraums jedoch nicht, ein Schutzkonzept zu wählen, bei dem der Schutz der Gesundheit der Nichtraucher im Ausgleich

(2) Effektives Schutzkonzept?

Folgende Aspekte könnten das bestehende staatliche Schutzkonzept als nicht hinreichend effektiv erscheinen lassen:

- Die gesetzliche Normierung nur generischer *Vertraulichkeit*sgebote – *statt* ausdrücklicher *Verschlüsselungs*pflichten – könnte sich als unzureichende materiellrechtliche Ausgestaltung der Schutzpflicht aus dem Fernmeldegeheimnis erweisen.
- Ein Schutzkonzept ist nur dann effektiv, wenn es auch über wirksame Kontrollmechanismen verfügt. Organisation und Verfahren der Überwachung der Normbefolgung könnten hier unzureichend sein.

  „Die konkrete gesetzliche Umsetzung der Schutzpflicht erfordert eine sorgfältige Analyse und Bewertung der Eignung der schon vorhandenen sowie der erwogenen Mechanismen, und zwar sowohl im Hinblick auf den materiellen Pflichtgehalt der Schutzregelungen als auch bezüglich Organisation und Verfahren in ihrer Überwachung."[1375]

(a) Effektive materiellrechtliche Ausgestaltung?

Zunächst müsste die einfachgesetzliche Ausgestaltung der grundrechtlichen Schutzpflichten dem Effektivitätsgebot genügen. Einfachgesetzliche Normen zur Umsetzung der grundrechtlichen Vertraulichkeitsgewährleistung aus dem Fernmeldegeheimnis sind vorhanden. Zu prüfen ist, ob die Schaffung von *Vertraulichkeits*erfordernissen zum Schutz des Fernmeldegeheimnisses hinreichend effektiv ist, oder ob allein die Schaffung ausdrücklicher *Verschlüsselungs*gebote effektiven Schutz gewährleistet.[1376]

(aa) Zulässigkeit der Verwendung unbestimmter Rechtsbegriffe

Grundsätzlich ist die gesetzgeberische Technik der Verwendung abstrakter und damit ausfüllungsbedürftiger (Rechts-)Begriffe in Gesetzen sowohl rechtsdogmatisch anerkannt[1377] als auch praxiserprobt.[1378] Insbesondere im Bereich des Technikrechts ist wegen der ihm innewohnenden Dynamik die Verweisung auf den „Stand der

mit den Freiheitsrechten der Gaststättenbetreiber und der Raucher weniger stringent verfolgt wird."

1375 *Brüning/Helios,* Jura 2001, 155, 162.

1376 Für die Normen, in denen eine explizite Verschlüsselungspflicht enthalten ist, bestehen hinsichtlich der Effektivität der Ausgestaltung natürlich keine Bedenken.

1377 *Schulze-Fielitz*, in: *Dreier,* GG, Art. 20 (Rechtsstaat), Rn. 133 mit vielen weiteren Nachweisen; *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 154.

1378 Sie ist darüber hinaus einer Rechtsordnung, die – wie insbesondere der deutsche Rechtskreis – von der Pandektenwissenschaft geprägt ist, in besonderem Maße inhärent. Eine Rechtsordnung aus dem Kreis des scholastisch geprägten, kontinentaleuropäischen *`civil law´* ist – im Gegensatz zum *`common law´* mit seinem eher forensischen Ansatz – naturgemäß verstärkt auf die Verwendung abstrakter Rechtsgriffe angewiesen.

Technik“, den „Stand von Wissenschaft und Technik“ oder die „allgemein anerkannten Regeln der Technik“ äußerst verbreitet:[1379]

> „Um die Erkenntnisse und Entwicklungen von Wissenschaft und Technik im Wege einer Normgebung, die damit Schritt hält, rechtlich verbindlich werden zu lassen, stehen dem Gesetzgeber grundsätzlich mehrere Möglichkeiten zur Verfügung. Sie haben, trotz der zwischen ihnen bestehenden Unterschiede, eines gemeinsam: Durch die Verwendung unbestimmter Rechtsbegriffe werden die Schwierigkeiten der verbindlichen Konkretisierung und der laufenden Anpassung an die wissenschaftliche und technische Entwicklung mehr oder weniger auf die administrative und – soweit es zu Rechtsstreitigkeiten kommt – auf die judikative Ebene verlagert. Behörden und Gerichte müssen mithin das Regelungsdefizit der normativen Ebene ausgleichen.“[1380]

Die grundsätzliche Zulässigkeit der Verwendung von unbestimmten Rechtsbegriffen oder Generalklauseln im Sinne einer Flexibilisierung von Normen hinsichtlich der technischen Entwicklung ist somit unstreitig. Dies gilt umso mehr, soweit (wie hier) der Staat selbst – in Form von Exekutive und Judikative – Adressat der Norm ist, da dieser umfassend der Bindung an Recht und Gesetz (Art. 20 III GG)[1381] und vor allem an die Grundrechte (Art. 1 III GG) unterliegt.[1382] So auch schon früh das BVerfG – allerdings für das Wirtschaftsverwaltungsrecht:

> „Die Vielheit der Verwaltungsaufgaben läßt sich nicht immer in klar umrissene Begriffe einfangen. Das gilt insbesondere für Eingriffsermächtigungen im Bereich der Wirtschaftsverwaltung. In diesem Bereich wird der Gesetzgeber nicht ohne Generalklauseln auskommen können. Er wird sich abstrakter und unbestimmter Formulierungen bedienen müssen, um die Verwaltungsbehörden in die Lage zu versetzen, ihren Aufgaben, den besonderen Umständen des einzelnen Falles und den schnell wechselnden Situationen des wirtschaftlichen Lebens gerecht zu werden.“[1383]

(bb) Nachbesserungspflicht?

Erscheint die Normierung von Vertraulichkeitsgeboten damit zunächst als adäquate Ausgestaltung der grundrechtlichen Schutzpflicht, die im Hinblick auf den gesetzgeberischen Einschätzungs-, Wertungs- und Gestaltungsspielraum kaum zu beanstanden wäre, stellt sich die Frage, ob sich wegen der gesetzgeberischen Beobachtungs- und Nachbesserungspflicht[1384] eine abweichende Beurteilung ergibt. Mag die Normierung generischer Vertraulichkeitsgebote etwa bei Erlass des Justizkommunikationsgesetzes (als dem zentralen Gesetz zur Einführung des elektronischen

1379 Vgl. zu den entsprechend der jeweils gewählten Terminologie abgestuften Anforderungen BVerfGE 49, 89, 135 f.
1380 BVerfGE 49, 89, 135 – Kalkar I.
1381 Vgl. insbesondere für die Schutzpflichtenerfüllung insoweit *Nitz*, Private und öffentliche Sicherheit, S. 385 ff.
1382 Im Gegensatz zum nicht grundrechtsgebundenen Individuum.
1383 BVerfGE 8, 274, 326.
1384 *Nitz*, Private und öffentliche Sicherheit, S. 388 f.

Rechtsverkehrs) als ausreichend erschienen sein, könnte sich mittlerweile eine Nachbesserungsverpflichtung ergeben haben:[1385]

> „Hat der Gesetzgeber eine Entscheidung getroffen, deren Grundlage durch neue, im Zeitpunkt des Gesetzeserlasses noch nicht abzusehende Entwicklungen entscheidend in Frage gestellt wird, dann kann er von Verfassungs wegen gehalten sein zu überprüfen, ob die ursprüngliche Entscheidung auch unter den veränderten Umständen aufrechtzuerhalten ist."[1386]

Eine solche Nachbesserungspflicht des Gesetzgebers ergibt sich zum einen, wenn sich nachträglich tatsächliche Veränderungen der Sachlage ergeben, etwa eine qualitative oder quantitative Zunahme der Beeinträchtigungen. Eine Nachbesserungspflicht ergibt sich aber auch dann, wenn bei unveränderter Sachlage neue Erkenntnisse bzgl. der tatsächlichen Gefährdungen vorliegen.[1387] Und zuletzt kann sich eine Nachbesserungspflicht ergeben, wenn sich vorhandene Schutzmaßnahmen de facto als unzureichend erwiesen haben.[1388] Für die Annahme einer gesetzgeberischen Nachbesserungsverpflichtung sprechen vorliegend folgende Argumente:

- Obwohl zahlreiche einfachgesetzliche Normen vorhanden sind, die den Schutz der Vertraulichkeit und – in verfassungskonformer Auslegung – den Einsatz von Verschlüsselung gebieten, ist das Bewusstsein – auch auf Seiten von Behörden – für die Bedeutung des Vertraulichkeitsschutzes erschreckend gering ausgeprägt. So ist etwa beim OVG Rheinland-Pfalz die Einreichung von Schriftsätzen in elektronischer Form nicht nur über das „Elektronische Gerichts- und Verwaltungspostfach" (EGVP)[1389] sowie per Web-Upload[1390] gestattet, sondern auch mittels einfacher E-Mail.[1391] Erforderlich ist jeweils nur eine qualifizierte elektronische Signatur (§ 55a I S. 3 VwGO). Ein paralleles Erfordernis der Gewährleistung von Vertraulichkeit – und nicht nur von Authentizität – enthält § 55a VwGO nicht.

1385 Siehe allgemein zur Nachbesserungspflicht *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 155; *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 268 ff. m.w.N.

1386 BVerfGE 49, 89, 130.

1387 Vgl. nochmal *Stüer/Loges,* NVwZ 2000, 9, 12: „Dieses bisher hingenommene Risiko kann aber durch neue Erkenntnisse für die Zukunft durch den Gesetzgeber neu bewertet und als nicht mehr hinnehmbar eingestuft werden, wenn dazu fachwissenschaftliche Erkenntnisse über ein erhöhtes Gefährdungsrisiko vorliegen […]"; siehe auch oben unter 3.a.cc) sowie *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 155.

1388 So auch *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 268.

1389 Beim Elektronischen Gerichts- und Verwaltungspostfach handelt es sich um eine Softwarelösung, in der alle technisch-organisatorischen Anforderungen implementiert sind. Weitere Informationen unter http://www.egvp. de (01.12.2008).

1390 Der Web-Upload erfolgt über die sog. „Virtuelle Poststelle". Über ein Webinterface können die einzureichenden Schriftsätze hochgeladen werden. Inwieweit dabei technisch eine Verschlüsselung der hochzuladenden Daten implementiert ist, ist unklar.

1391 Siehe die Landesverordnung über den elektronischen Rechtsverkehr mit den öffentlich-rechtlichen Fachgerichten vom 09.01.2008 (GVBl. S. 33).

Ein Vertraulichkeitsgebot ergibt sich zwar aus den allgemeinen datenschutzrechtlichen Normen, in diesem Fall § 9 Landesdatenschutzgesetz Rheinland-Pfalz,[1392] der in Abs. 2, S. 2, Nr. 4 insbesondere gebietet,

„zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, […]".

Alle Personen, die dienstlichen Zugang zu personenbezogenen Daten haben, werden nach § 8 II LDSG über die einzuhaltenden datenschutzrechtlichen Vorschriften unterrichtet und zu deren Einhaltung verpflichtet. Die soeben dargestellte Praxis zeigt aber, dass ein Datenschutzbewusstsein wenig ausgeprägt ist. Wird noch nicht mal das umfassende Vertraulichkeitsgebot tatsächlich erkannt und in der Praxis umgesetzt, folgt daraus, dass eine Problematisierung der Frage, wie im einzelnen die Vertraulichkeit zu gewährleisten ist, ob etwa in verfassungskonformer Auslegung der Einsatz von Verschlüsselungsverfahren erforderlich ist, regelmäßig nicht stattfindet.[1393] Dafür darf durchaus auch § 55a VwGO als ursächlich angesehen werden, der im Referentenentwurf vom 14.04.2003 in Abs. 1, S. 2 noch eine Verschlüsselungspflicht enthielt:

„Daten, die nach einem Gesetz oder ihrem Wesen nach geheim gehalten werden müssen, sind zu verschlüsseln."[1394]

Dabei verstärkt die Asymmetrie zwischen Schutz der Authentizität und Integrität einerseits und Schutz der Vertraulichkeit andererseits diesen Mangel an Datenschutzbewusstsein zusätzlich: Dadurch, dass das Erfordernis von Authentizität und Integrität unmittelbar in § 55a VwGO normiert ist, entsteht der Eindruck, damit seien alle wesentlichen Verfahrensanforderungen genannt; der aus den Datenschutzgesetzen kommende Vertraulichkeitsschutz wird vergessen.
Zusammenfassend ist festzuhalten, dass es häufig bereits an einem Bewusstsein für die Notwendigkeit von Vertraulichkeitsschutz fehlt. Eine verfassungskonforme Auslegung der entsprechenden Normen dahingehend, dass zu verschlüsseln ist, erfolgt in einer solchen Situation nicht. Dazu trägt auch die derzeitige gesetzgeberische Konzeption der entsprechenden einfachgesetzlichen Normen bei: Explizite Verschlüsselungspflichten sind selten; eine Vielzahl spezialgesetzlicher Normen fordert nur generisch den Schutz der Vertraulichkeit; das Datenschutzrecht, dass diese Mängel ausgleichen müsste, ist kompliziert, höchst

1392 Landesdatenschutzgesetz (LDSG) vom 05.07.1994 (GVBl, S. 293).

1393 Daher fruchtet hier das Argument, in verfassungskonformer Auslegung erfüllten die generischen Vertraulichkeitsgebote die staatliche Schutzpflicht (so *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 156), wenig. Mangelt es de facto an einer solchen notwendigen verfassungskonformen Auslegung, muss dieser Tatsache in irgendeiner Form Rechnung getragen werden. Die nur abstrakte Möglichkeit einer verfassungskonformen Auslegung kann für ein effektives Schutzkonzept nicht ausreichend sein.

1394 Siehe die Synopse des Referentenentwurfs vom 14.04.2003 und des Regierungsentwurfs vom 28.07.2004 unter https://www.edvgt.de/media/doc/SynopseJKomG.pdf (01.12.2008).

unübersichtlich und in seinen konkreten Anforderungen für Laien häufig unklar.[1395]

- Zugleich hat sich seit Inkrafttreten des ersten Bundesdatenschutzgesetzes (BDSG)[1396] am 01.02.1977 die Sachlage grundlegend geändert, und ist heute die Vertraulichkeit qualitativ und quantitativ vollkommen anderen Beeinträchtigungen ausgesetzt. Das allgemeine Datenschutzrecht wird insoweit stellvertretend für die Gesamtheit der speziellen Datenschutznormen betrachtet.[1397] Seit der Schaffung des BDSG hat sich der *rechtliche Rahmen* des technischen und organisatorischen Datenschutzes *kaum verändert*.[1398] Im selben Zeitraum haben sich nicht nur *umfassende technische Veränderungen* (Miniaturisierung, Ubiquität, zunehmend kabellose Übertragungswege), sondern auch *grundlegende gesellschaftliche Veränderungen* ergeben: Verlagerung von Alltagsgeschäften, steigende Betroffenheit sensibler Daten, Permanenz von Daten, Verkettbarkeit von Daten, zunehmende Sozialüblichkeit, verbesserte Auswertungsmöglichkeiten, qualifizierte Angriffsszenarien; zu den Einzelheiten s.o. in Teil 3 unter

1395 So kritisiert etwa *Simitis*, in: *Simitis,* BDSG, Einl., Rn. 101 mit aller Deutlichkeit: „Eine auffällig exzessive Verwendung von Generalklauseln und unbestimmten Rechtsbegriffen, die Überfrachtung mit Ausnahmeregelungen, deren Tragweite nur schwer, wenn überhaupt abzuschätzen ist, komplizierte, kaum nachzuvollziehende Verweisungen und eindeutig nicht aufeinander abgestimmt Vorschriften machen das Gesetz unleserlich und die Interpretation vollends zum Risiko." Ähnlich auch *Hoffmann-Riem,* AöR 1998, 513, 516: „Komplizierte Anwendungsregelungen, verschachtelte Verweisungen, vielfältige Bereichssonderregeln und offen formulierte Abwägungsermächtigungen prägen das Bild. Das Datenschutzrecht ist heutzutage wohl nicht einmal mehr für Experten leicht verständlich und praktikabel." Vgl. eine gute Zusammenfassung über die Mängel des bestehenden Datenschutzrechts bei Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts, verfügbar unter: http://www.computerundrecht.de/media/gutachten.pdf (02.12.2008), S. 22 ff.

1396 Bundesdatenschutzgesetz vom 01.02.1977 (BGBl. I, 201), einen Überblick über die Geschichte des Datenschutzrechts gibt *Simitis*, in: *Simitis,* BDSG, Einl., Rn. 1 ff.

1397 Wie bereits der hier gegebene kurze Überblick über Normen, die „Vertraulichkeit" oder „Schutz vor unbefugter Kenntnisnahme" vorschreiben, gezeigt hat, gibt es eine immense Zahl an bereichsspezifischen Sonderregelungen zum Vertraulichkeitsschutz. Zumeist handelt es sich dabei um spezielles Datenschutzrecht, da es um den Schutz personenbezogener Daten geht. Normen, die Vertraulichkeit oder Verschlüsselung vorschreiben zum Schutz nicht personenbezogener Daten sind demgegenüber äußerst selten. Ein Beispiel könnte § 23, S. 1 TEHG sein, da hier wohl hauptsächlich unternehmensbezogene Daten übermittelt werden. Hier scheint der Schutz von Betriebs- und Geschäftsgeheimnissen eher im Vordergrund zu stehen. Gleichwohl ist auch hier die Übermittlung personenbezogener Daten denkbar. Ganz überwiegend handelt es sich bei den Vertraulichkeitsgeboten um solche zum Schutze personenbezogener Daten, also um Datenschutzrecht. Da im Rahmen dieser Arbeit zum einen nicht jede Norm gesondert betrachtet werden kann und zum anderen diese speziellen Datenschutzreglungen auf dem allgemeinen Datenschutzrecht basieren (in weiten Teilen sogar Regelungen des allgemeinen Datenschutzrechts nur – in leicht abgewandelter Form – wiederholen; vgl. dazu Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts, verfügbar unter: http://www.computerundrecht.de/media/gutachten.pdf (02.12. 2008), S. 30), wird hier maßgeblich auf das allgemeine Datenschutzrecht abgestellt.

1398 Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts, verfügbar unter: http://www.computerundrecht.de/media/gutachten.pdf (02.12.2008), S. 23.

A.III.1.d.aa). Zusammenfassend werden zum einen immer mehr Daten erhoben und gespeichert, denen zum anderen immer größere Bedeutung zukommt, da sie nicht nur die Bildung von Persönlichkeits-, Konsum- oder sonstigen Profilen erlauben, sondern über die Profilbildung hinaus direkten Einfluss auf das Leben der Betroffenen haben (etwa beim Einsatz von Scoringverfahren im Rahmen der Kreditvergabe, der Generierung von Kundenprofilen, die über die Gewährung oder Nicht-Gewährung einer besonders bevorzugten Behandlung entscheiden, usw.). Die Nutzung von Informations- und Kommunikationstechnologien ist dabei längst nicht mehr nur für die Wirtschaft interessant, sondern in der Gesellschaft allgegenwärtig. Dies bedeutet für den Einzelnen, dass er sich diesen Technologien immer weniger effektiv entziehen kann.

Diese Veränderungen treffen auch die Vertraulichkeit der Telekommunikation. Dachte 1977 noch niemand an E-Mails,[1399] handelt es sich heute um ein alltägliches Massenphänomen. Die daraus resultierenden Vertraulichkeitsgefährdungen sind mit den Vertraulichkeitsgefahren der herkömmlichen Sprachtelekommunikation nicht mehr vergleichbar. Qualitativ wie quantitativ ergeben sich völlig andere Möglichkeiten der Beeinträchtigung von Vertraulichkeit.

- Die Kombination eines extrem stark angestiegenen Gefährdungspotentials für die Vertraulichkeit von Datenkommunikation mit einem mangelhaften (öffentlichen wie privaten) Bewusstsein für die Notwendigkeit und Wichtigkeit des Vertraulichkeitsschutzes spricht klar für eine gesetzgeberische Nachbesserungspflicht. Selbst wenn man dem Gesetzgeber bezüglich der Einschreitensschwelle (also der Frage, wann Änderungen der Sachlage so gravierend sind, dass sich diese zu einer Nachbesserungs*pflich*t verdichten) sowie der Art der Überwachung der staatlichen Schutzpflichterfüllung (also der Frage, wann[1400] die zuständigen staatlichen Organe eine eventuelle Nachbesserung *prüfen* müssen) einen Ermessensspielraum zubilligen würde, ergäbe sich nicht anderes. Die Veränderung des gesellschaftlichen Alltags durch die zunehmende Durchdringung aller Lebensbereiche von Informations- und Kommunikationstechnologien ist offensichtlich – eine Prüfung oder Überwachung der Schutzpflichterfüllung ist nicht notwendig, um diese Veränderungen zu erkennen. Es herrscht breiter Konsens über die Notwendigkeit einer grundlegenden Reform der Datenschutznormen – gerade auch im Hinblick auf die genannten Entwicklungen.[1401] Daher steht zum einen fest, dass eine Nachbesserungspflicht besteht. Die Kritik am

1399 In Deutschland wurde die erste E-Mail laut Wikipedia, E-Mail, Version vom 01.12.2008, 13.46 Uhr, verfügbar unter: http://de.wikipedia.org/w/index.php?title=E-Mail&oldid=53630851 im Jahr 1984 empfangen. Sicher war jedenfalls die zukünftige massenhafte Individualkommunikation mittels allgemein zugänglicher Netze noch nicht ansatzweise zu erahnen.

1400 „Wann" bezieht sich hier sowohl auf den Zeitpunkt als auch auf die Schwere des Anlasses, sprich: Zu welchem Zeitpunkt muss der Gesetzgeber tätig werden? Wie gravierend müssen die tatsächlichen Veränderungen sein, damit der Gesetzgeber tätig werden muss?

1401 Vgl. insoweit nur das vom Bundesministerium des Innern in Auftrag gegebene Gutachten aus dem Jahr 2001: Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts, verfügbar unter: http://www.computerundrecht.de/media/gutachten.pdf (02.12.2008).

geltenden Datenschutzrecht ist darüber hinaus so alt, dass auch in zeitlicher Hinsicht ein Ermessensspielraum überschritten wäre.

Der Gesetzgeber ist daher zur Nachbesserung der Gestaltung des Vertraulichkeitsschutzes durch staatliche Behörden verpflichtet.[1402] Die konkrete Verpflichtung, statt allgemeiner Vertraulichkeitsgebote dezidiert Verschlüsselung zu fordern, kann allerdings nicht aus dieser Nachbesserungspflicht abgeleitet werden: Der Missstand des mangelnden behördlichen Datenschutzbewusstseins könnte auch auf andere Weise – etwa durch besondere Schulungen sowie die Aufnahme der „Vermittlung von Medienkompetenz im Umgang mit Informations- und Kommunikationstechnologien“[1403] in die Curricula der schulischen und beruflichen Aus- und Weiterbildung – behoben werden. Dies sind aber keine Maßnahmen, die dem *Gesetzgeber*, an den sich die Nachbesserungspflicht richtet, zur Verfügung stehen. Der Gesetzgeber kann nur gesetzgeberische Maßnahmen ergreifen. Das bedeutet, er könnte – wie hier diskutiert – Vertraulichkeitserfordernisse stärker auch in Spezialgesetzen festschreiben sowie dabei auch auf eventuelle Verschlüsselungspflichten hinweisen.[1404] Er könnte auch das Datenschutzrecht umfassend reformieren und für größere Klarheit sowie höhere Praktikabilität sorgen. Oder er könnte die besagten Schulungsmaßnahmen gesetzlich vorschreiben.

Allein diese kurze Darstellung verdeutlicht, dass auch im Bereich der Nachbesserungspflichten dem Gesetzgeber erneut ein *Einschätzungs-, Wertungs- und Gestaltungsspielraum* zukommt.[1405] Einzige Zusatzanforderung, die man bei einer Nachbesserungspflicht im Verhältnis zur Erstgestaltung eines staatlichen Schutzkonzepts wird treffen können, dürfte eine qualifizierte Auseinandersetzung mit den Tatsachen sein, die das bisherige Schutzkonzept als defizitär erscheinen lassen. Aber auch hier wird man wohl jede einigermaßen vernünftige Überlegung des Gesetzgebers hinzunehmen haben.

1402 Insoweit kann hier die Frage von Selbstschutzmöglichkeiten des Grundrechtsberechtigten (vgl. dazu *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 142 sowie unten unter 5.a.) keine Rolle spielen: Die Grundrechtsberechtigten mögen zwar im Verhältnis zueinander vom Staat auf zumutbare Selbstschutzmaßnahmen verwiesen werden können, der Staat selbst kann sich aber für eigenes Handeln nicht darauf zurückziehen, der Einzelne müsse sich eben selbst schützen. Darüber hinaus hat der Einzelne in vielen Konstellationen keinen Einfluss auf den Vertraulichkeitsschutz, etwa bei Datenübermittlungen zwischen zwei Behörden oder bei vom Staat gestalteten E-Government-Anforderungen – sehen diese etwa den Versand verschlüsselter E-Mails nicht vor, nutzen dem Einzelnen theoretisch bestehende Selbstschutzoptionen möglich.

1403 So etwa der Antrag der Bundestagsfraktion von Bündnis 90/Die Grünen zum Schutz der Privatsphäre in sozialen Netzwerken vom 11.02.2009 unter Ziffer II.3, BT-Drs. 16/11920, S. 4.

1404 Wie dies etwa im oben genannten Bespiel von § 89a VIII AufenthG geschehen ist: „Die beteiligten Stellen haben dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten gewährleisten; im Falle der Nutzung allgemein zugänglicher Netze sind dem jeweiligen Stand der Technik entsprechende Verschlüsselungsverfahren anzuwenden.“

1405 So auch *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 269.

Dies spricht im Ergebnis gegen die Deduktion einer konkreten Schutzmaßnahme aus dem staatlichen Nachbesserungsauftrag. Unabhängig von der Frage, ob sich aus dem objektiv-rechtlichen Schutzpflichtenauftrag überhaupt ein subjektives Recht des Einzelnen (siehe dazu sogleich unter 5.b.) auf Nachbesserung ergibt, kann ein solches jedenfalls nur in Form einer auf eine bestimmte Maßnahme gerichteten Klage gerichtlich geltend gemacht werden. Ein derartiger materieller Anspruch auf den Erlass einer bestimmten Nachbesserungsmaßnahme besteht hier wegen des Einschätzungs-, Wertungs- und Gestaltungsspielraums des Gesetzgebers nicht. Mag auch der Gesetzgeber zur Nachbesserung bezüglich der Erfüllung des Schutzpflichtenauftrags verpflichtet sein, ist dies aber nicht auf gerichtlichem Wege einklagbar.

(b) Effektive Überwachung der Einhaltung von Vertraulichkeitsgeboten?

Weiter kann ein staatliches Schutzkonzept nur dann als effektiv angesehen werden, wenn dieses wirksamer Kontrolle unterliegt.[1406] Organisation und Verfahren der Überwachung der Umsetzung von Schutzmaßnahmen müssen ausreichend sein.[1407] Insgesamt geht es also darum, dass die Vertraulichkeitsgebote auch wirksam *durchgesetzt* werden und keine (gravierenden) Vollzugsdefizite bestehen.

In der Literatur[1408] wurden die folgenden Kategorien von Vollzugsdefiziten auf Verwaltungsebene herausgearbeitet:

- Zielwidriges Behördenhandeln[1409]
- Unzureichende Kontrolle des Verhaltens des Normadressaten
- Sanktionsmängel

Für den hier relevanten Bereich des technischen und organisatorischen Datenschutzes könnten vor allem eine unzureichende Kontrolle der Normbefolgung sowie ein Mangel an Sanktionen gegen normverletzende Adressaten vorliegen.

(aa) Sanktionsmängel

Für die Überwachung der Einhaltung der datenschutzrechtlichen Bestimmungen sind grundsätzlich der Bundesdatenschutzbeauftragte bzw. die entsprechenden Landesdatenschutzbeauftragten in ihrem jeweiligen Zuständigkeitsbereich – je nachdem, wer datenverarbeitende Stelle ist – zuständig, vgl. etwa § 24 I BDSG:

> „Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz.“[1410]

1406 Vgl. zu Bedeutung und Folgen von Vollzugsmängeln auch die Ausführungen zu symbolischem Recht in Teil 3 unter C.

1407 *Möstl,* DÖV 1998, 1029, 133; *Brüning/Helios,* Jura 2001, 155, 162.

1408 *Holtschneider*, Normenflut und Rechtsversagen, S. 162 f.

1409 Sei es durch Nichtanwendung restriktiver Normen, mangelnder Ausschöpfung gegebener Rahmenregelungen oder zielwidrige Ermessensausübung, vgl. *Holtschneider*, Normenflut und Rechtsversagen, S. 162.

Als Instrumente stehen dem Bundesdatenschutzbeauftragten die Beanstandung (§ 25 I BDSG), die Erwähnung im Tätigkeitsbericht (§ 26 I BDSG) sowie die Abgabe von Empfehlungen und Beratung (§ 26 III BDSG) zu. Der Bundesdatenschutzbeauftragte erstellt zudem Gutachten und erstattet Bundestag und Bundesregierung Bericht (§ 26 II S. 1 BDSG). Er kann sich seinerseits jederzeit an den Bundestag wenden (§ 26 III S. 3 BDSG). Jenseits dieser eher „weichen" Instrumente gibt es in den §§ 43 und 44 BDSG umfangreiche Ordnungswidrigkeiten- und Straftatenkataloge. Für die Ahndung von Ordnungswidrigkeiten und Straftaten ist der Bundesdatenschutzbeauftragte aber nicht selbst zuständig.[1411] Er kann gegebenenfalls bei der jeweils zuständigen Stelle Strafantrag stellen (§ 44 II S. 2 BDSG) bzw. die Ordnungswidrigkeit melden.

Geht es – wie bei der Frage nach der Gewährleistung von Vertraulichkeit – um das Fehlen technisch-organisatorischer Datenschutzmaßnahmen, ist aber ohnehin keiner der Bußgeldtatbestände einschlägig. Es bleibt in diesem Bereich daher allein bei den oben genannten Kontrollinstrumenten. Dabei sind nicht nur Empfehlung und Beratung ohne rechtliche Wirkung, sondern weitestgehend auch die Beanstandung.[1412] Sie löst nur die Pflicht aus, eine Stellungnahme abzugeben.[1413] Unmittelbare Sanktionen oder Zwangsmaßnahmen zur Durchsetzung der Beanstandung gibt es nicht.[1414] Der Bundesdatenschutzbeauftragte kann darüber hinaus den Bundestag anrufen, der Bundesregierung entsprechende Empfehlungen geben oder den Vorgang in seinen Tätigkeitsbericht aufnehmen.[1415]

Daher ist für den technisch-organisatorischen Datenschutz das Vorliegen von Sanktionsmängeln zu bejahen:[1416] [1417]

1410 Jeweils entsprechende Normen gibt es auf Landesebene, etwa in Hessen § 24 I S. 1 HDSG. Auch die im Folgenden genannten weiteren Normen des BDSG finden regelmäßig auf Landesebene eine Entsprechung, auf die nicht jeweils gesondert eingegangen wird.

1411 Vgl. die Einzelheiten zu den Zuständigkeiten sowohl auf Bundes- als auch auf Landesebene bei *Gola/Schomerus,* BDSG, § 43, Rn. 28.

1412 *Dammann*, in: *Simitis,* BDSG, § 25, Rn. 2.

1413 *Dammann*, in: *Simitis,* BDSG, § 25, Rn. 11.

1414 Nach *Dammann*, in: *Simitis,* BDSG, § 25, Rn. 21 ist das Beanstandungsverfahren geradezu als „Gegenmodell" zur gerichtlichen Auseinandersetzung ausgestaltet.

1415 *Dammann*, in: *Simitis,* BDSG, § 25, Rn. 15.

1416 Für diese Einschätzung spricht auch eine Gesetzgebungsinitiative des Bundesministerium des Innern, wonach dem BSI als zusätzliche Aufgabe „die Prüfung und Bestätigung der Konformität im Bereich der IT-Sicherheit von informationstechnischen Systemen" übertragen werden soll; heise online vom 12.12.2008, Innenministerium: Mehr Biss für die IT-Sicherheit des Bundes, verfügbar unter: http://www.heise.de/newsticker/Innenministerium-Mehr-Biss-fuer-die-IT-Sicherheit-des-Bundes--/meldung/120 317 (15.12.2008).

1417 Ähnlich scheint dies das BVerfG zu sehen, dass in seiner Entscheidung zur Vorratsdatenspeicherung ein verfassungsrechtliches Gebot der angemessenen Sanktionierung von Verstößen gegen die Datensicherheit aus dem Fernmeldegeheimnis deduziert: „Verfassungsrechtlich geboten sind weiterhin eine für die Öffentlichkeit transparente Kontrolle unter Einbeziehung des unabhängigen Datenschutzbeauftragten sowie ein ausgeglichenes Sanktionensystem, das auch Verstößen gegen die Datensicherheit ein angemessenes Gewicht beimisst."; BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08 et al., Rn. 225.

- Verstöße gegen die Gebote des technisch-organisatorischen Datenschutzes werden weder durch Straftat- noch durch Ordnungswidrigkeitentatbestände geahndet.
- Das „schärfste“ Sanktionsinstrument ist die Beanstandung, welche aber lediglich eine Verpflichtung zur Stellungnahme nach sich zieht. Diese Verpflichtung kann aber nicht gerichtlich oder in sonstiger Weise zwangsweise durchgesetzt werden. Auch eine Veränderung der beanstandeten Situation kann nicht rechtlich durchgesetzt werden.
- Als Sanktionsmaßnahmen bleiben somit die „Prangerwirkung“ einer Erwähnung im Tätigkeitsbericht sowie eine Intervention des Bundestags oder der Bundesregierung. Damit liegen nur äußerst schwache Sanktionsmöglichkeiten vor.

Dem Bundesdatenschutzbeauftragten stehen im Ergebnis lediglich „weiche“ Kontrollinstrumente zur Verfügung, die eher auf Zusammenarbeit, denn auf Konfrontation, streitige Entscheidung und zwangsweise Durchsetzung angelegt sind.[1418] Idee einer solchen Konzeption dürfte gewesen sein, dadurch ein wachsendes eigenes Datenschutzbewusstsein bei den datenverarbeitenden Stellen zu schaffen. Letzteres ist jedoch immer noch (zu) wenig ausgeprägt. Für den Bereich „Verschlüsselung“ konstatiert der Bundesdatenschutzbeauftragte in seinem 21. Tätigkeitbericht:

> „Leider musste ich bei Beratungen und Kontrollen immer wieder feststellen, dass nur in wenigen Fällen entsprechende Verfahren eingesetzt werden. So musste ich zum Beispiel darauf hinweisen, dass insbesondere sensible Daten (z. B. Personal- und Sozialdaten, Daten über den Gesundheitszustand) in besonderer Weise geschützt werden müssen. Häufig wird mir das Argument entgegengehalten, die Verschlüsselung sei mit unzumutbarem Aufwand und mit zusätzlichen Kosten verbunden. Hierzu ist festzustellen, dass inzwischen effektive Verschlüsselungsverfahren zur Verfügung stehen, die sich verhältnismäßig einfach einsetzen lassen. Außerdem sollte nicht außer Acht bleiben, dass der Datenmissbrauch ein erhebliches materielles Schadenspotenzial aufweist und tief greifende Verletzungen des Rechts auf informationelle Selbstbestimmung zur Folge haben kann.“[1419]

(bb) Unzureichende Kontrolle

Es könnte darüber hinaus bereits auf der vorangehenden Stufe, bei der Feststellung von Datenschutzverstößen, Vollzugsdefizite geben. Eine unzureichende Kontrolle des Verhaltens des Normadressaten kann sich zum einen aus generell fehlenden

1418 Zu den Vorteilen, aber auch den Gefahren solcher Kooperationsstrategien siehe *Holtschneider*, Normenflut und Rechtsversagen, S. 210 ff., der von „informalem Verwaltungshandeln“ spricht. Als Gefahren nennt er insbesondere den möglichen Ausschluss von Rechtsschutz, die Bevorzugung von mächtigen gegenüber weniger mächtigen Interessengruppen, dadurch bedingt die mangelnde Transparenz, die Gefahr der Einigung auf dem kleinsten Nenner.

1419 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Tätigkeitsbericht 2005-2006, verfügbar unter: http://www.bfdi.bund.de/cln_027/nn_531940/SharedDocs/Publikationen/Taetigkeitsberichte/21-Taetigkeitsbericht-2005-2006,templateId=raw,property=publicationFile.pdf/21-Taetigkeitsbericht-2005-2006. pdf (09.12.2008), S. 47.

Kontrollinstanzen oder aus de facto nicht stattfindenden Kontrollen ergeben.[1420] Dabei erfordern Kontrollen die entsprechenden Ressourcen.[1421]

Eine Kontrollinstanz ist mit dem Bundes- bzw. dem jeweils zuständigen Landesdatenschutzbeauftragten für den öffentlichen Bereich vorhanden. Die zur Erfüllung dieser Kontrollaufgabe notwenigen Personal- und Sachmittel werden dem Bundesdatenschutzbeauftragten nach § 22 V S. 3 BDSG zur Verfügung gestellt. Inwieweit diese Personal- und Sachausstattung tatsächlich zu einer effektiven Aufgabenerfüllung ausreichend ist, kann nicht abschließend beurteilt werden. Angesichts der umfangreichen Aufgaben des Bundesdatenschutzbeauftragten[1422] scheint die Personalausstattung von ca. 70 Mitarbeitern[1423] allerdings nicht ausreichend.[1424]

1420 Darüber hinaus können sich nach jüngster Rechtsprechung des EuGH (vgl. EuGH, Urteil vom 09.03.2010, Rs. C-518/07) Kontrolldefizite auch aus einer fehlenden Unabhängigkeit der für die Beaufsichtigung der Einhaltung der Datenschutzregelungen zuständigen Stellen ergeben. Der EuGH hat ausgeführt, dass bei einer fehlenden Unabhängigkeit der Kontrollinstanzen (in dem Fall der Aufsichtsbehörden für den nicht-öffentlichen Bereich) nicht ausgeschlossen werden kann, dass von staatlicher Seite ein Interesse an der Nichteinhaltung von Datenschutzvorschriften besteht: „Es lässt sich aber nicht ausschließen, dass die Aufsichtsstellen, die Teil der allgemeinen Staatsverwaltung und damit der Regierung des jeweiligen Landes unterstellt sind, nicht zu objektivem Vorgehen in der Lage sind, wenn sie die Vorschriften über die Verarbeitung personenbezogener Daten auslegen und anwenden. Die Regierung des betroffenen Landes hat nämlich, wie der EDSB in seinen Erklärungen hervorhebt, möglicherweise ein Interesse an der Nichteinhaltung der Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, wenn es um die Verarbeitung solcher Daten im nichtöffentlichen Bereich geht. Sie kann selbst involvierte Partei dieser Verarbeitung sein, wenn sie davon betroffen ist oder sein könnte, z. B. im Fall einer Kooperation von öffentlichen und privaten Stellen oder im Rahmen öffentlicher Aufträge an den privaten Bereich. Außerdem könnte sie ein besonderes Interesse haben, wenn sie für bestimmte ihrer Aufgaben, insbesondere zu Zwecken der Finanzverwaltung oder der Strafverfolgung, Zugang zu Datenbanken benötigt oder ein solcher Zugang einfach nur sachdienlich ist. Im Übrigen könnte diese Regierung auch geneigt sein, wirtschaftlichen Interessen den Vorrang zu geben, wenn es um die Anwendung der genannten Vorschriften durch bestimmte Unternehmen geht, die für das Land oder die Region wirtschaftlich von Bedeutung sind.“; EuGH, Urteil vom 09.03.2010, Rs. C-518/07, Rn. 34 f.

1421 *Holtschneider*, Normenflut und Rechtsversagen, S. 163.

1422 Vgl. insoweit nur das Organigramm unter http://www.bfdi.bund.de/cln_118/DE/Dienststelle/Organisation/organisation_node.html (03.08.2009).

1423 Zahlen nach http://www.bfdi.bund.de/cln_118/DE/Dienststelle/Aufgaben/Aufgaben_node.html (03.08.2009).

1424 So auch jüngst der „Düsseldorfer Kreis“, ein informelles Gremium der obersten Aufsichtsbehörden für den nicht-öffentlichen Bereich, in seinem Beschluss vom 13./14.11.2008 „Novellierung des Bundesdatenschutzgesetzes in den Bereichen Adressenhandel, Werbung und Datenschutzaudit“ (verfügbar unter http://www.bfdi.bund.de/cln_027/nn_1207036/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/DuesseldorferKreis/141108Adresshandel,templateId=raw,property=publicationFile.pdf/141108Adresshandel.pdf (10.12.2008)), der neben adäquaten Kontroll- und Sanktionsmöglichkeiten (!) eine angemessene Ausstattung der Aufsichtsbehörden forderte. Siehe zu (Personal-)Ausstattung und Arbeitsbelastung der Aufsichtsbehörden für den nicht-öffentlichen Bereich auch Xamit Bewertungsgesellschaft, Datenschutzbarometer 2009, verfügbar unter: http://www.xamitleistungen.de/downloads/Xamit Datenschutzbarometer2009.pdf (03.12.2009), S. 26 ff., die zu einer rechnerischen Kontroll-

(c) Zusammenfassung

Im Ergebnis ist festzuhalten, dass es sowohl bei der Feststellung von Datenschutzverstößen als auch bei der Sanktionierung dieser Verstöße erhebliche Vollzugsdefizite gibt.[1425] Die Einhaltung von Vertraulichkeitsgeboten wird somit nicht effektiv überwacht; das staatliche Schutzkonzept zur Gewährleistung der Vertraulichkeit von Telekommunikation gem. Art. 10 I GG nicht wirksam kontrolliert.[1426] Jenseits dieses Kontrolldefizits scheint das Datenschutzrecht insgesamt als nachbesserungsbedürftig, gerade auch hinsichtlich des Vertraulichkeitsschutzes. Eine konkrete Verpflichtung des Gesetzgebers, verstärkt explizite Verschlüsselungspflichten zu normieren, kann daraus wegen des gesetzgeberischen Einschätzungs-, Wertungs- und Gestaltungsspielraums jedoch nicht abgeleitet werden. Trotzdem bleibt es bei einer grundsätzlichen Nachbesserungspflicht des Gesetzgebers, die aber – mangels einer Ermessensreduktion auf Null, die zu einer ganz bestimmten Nachbesserungsmaßnahme verpflichten würde – klageweise nicht durchgesetzt werden kann.[1427] Ein effektives Schutzkonzept liegt somit nicht vor.

frequenz von einer Kontrolle pro Unternehmen alle 39.400 Jahre kommen. Da zum Teil (vgl. ausführlich dazu *Gola/Schomerus,* BDSG, § 38, Rn. 29) die Landesdatenschutzbeauftragten auch Aufsichtsbehörde für den nicht-öffentlichen Bereich sind, liegt die Annahme einer insgesamt nicht ausreichenden Ausstattung nahe. Ähnlich äußerte sich auch der scheidende Datenschutzbeauftragte Lubomierski, allerdings für den privaten Bereich. Die für die Kontrolle des privaten Bereichs vorgesehenen drei Mitarbeiter könnten nur den ca. 700 eingehenden konkreten Hinweisen nachgehen – eine anlassunabhängige Kontrolle sei daneben nicht möglich; vgl. heise online vom 26.12.2008, "Sitzen in der Technikfalle" - Hamburgs Datenschützer zieht Bilanz, verfügbar unter: http:// www.heise.de/newsticker/Sitzen-in-der-Technikfalle-Hamburgs-Datenschuetzer-zieht-Bilanz--/meldung/120921 (29.12.2008). Gayk, Datenschutzkontrolle der Beschäftigtenkontrolleuere, Vortrag im Rahmen der Sommerakademie des ULD Schleswig-Holstein am 31.08.2009, verfügbar unter: https://www.datenschutzzentrum.de/sommerakademie/2009/sak09-gayk-datenschutzkontrolle-der-beschaeftigten kontrolleure.pdf (02. 09.2009), S. 3 nannte jüngst für Nordrhein-Westfalen einen „Betreuungsschlüssel" von 1 zu 24.000 (Unternehmen). Hinzu kommt die Kontrolle der öffentlichen Stellen.

1425 *Trute*, Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57, 216, 262 hält die gesamte administrative Kontrollstrategie des Datenschutzrechts für unzureichend angesichts der Ubiquität der Informationsvorgänge. Ob sein Gegenvorschlag, stärker auf freiwillige Selbstregulierung und Anreizsysteme zu setzen, das Effektivitätsdefizit beseitigen würde, ist allerdings ebenso zweifelhaft. Das letzte Jahrzehnt hat eigentlich eher gezeigt, dass die „weichen" Ansätze noch nicht mal bei öffentlichen, geschweige denn bei nicht-öffentlichen Stellen ausreichen.

1426 Mangelhafte Kontrolle der Einhaltung des BDSG rügen laut heise online vom 11.12.2008, Schäubles Datenschutzgesetz geht SPD und FDP nicht weit genug, verfügbar unter: http://www.heise.de/newsticker/Schaeubles-Datenschutzgesetz-geht-SPD-und-FDP-nicht-weit-genug--/meldung/120292 (12.12.2008) auch Sabine Leutheusser-Schnarrenberger (FDP) und Dieter Wiefelspütz (SPD). Als Abhilfemaßnahme befürwortete Wiefelspütz dabei eine personelle Stärkung des Bundesdatenschutzbeauftragten.

1427 Ähnliches gilt für die Frage nach einer Staatshaftung aus § 839 BGB i.V.m. Art. 34 GG auf Grund legislativen Unterlassens: Jenseits der umstrittenen Frage nach Existenz und Umfang einer staatlichen Haftung für legislatives Unrecht (vgl. etwa *Wieland*, in: *Dreier*, GG, Art. 34, Rn. 49 ff.; *v. Danwitz*, in: *v. Mangoldt/Klein/Starck*, GG, Art. 34, Rn. 110 ff.) kommt eine

d. Ergebnis

Damit liegt im Ergebnis ein Verstoß gegen das Untermaßverbot vor. Das staatliche Schutzkonzept ist aufgrund von Vollzugsdefiziten ineffektiv. Auf eine Abwägung der widerstreitenden Rechtspositionen im Rahmen der Angemessenheit kommt es nicht mehr an.

5. Folgen ineffektiven staatlichen Schutzes

Zu prüfen bleibt, ob und, wenn ja, welche Folgen sich aus dem ineffektiven staatlichen Schutz des Fernmeldegeheimnisses (Art. 10 I GG) ergeben. Grundsätzlich sind für den betroffenen Grundrechtsberechtigten zwei Möglichkeiten denkbar:

- Betroffene Grundrechtsberechtigte könnten aufgrund des mangelnden staatlichen Schutzes zu Selbstschutzmaßnahmen greifen. Insofern stellt sich die Frage, inwieweit derartige Selbstschutzmaßnahmen rechtlich zulässig sind und in welchem Verhältnis der eigenverantwortliche Schutz durch den Grundrechtsberechtigten selbst zu dem durch den Staat geleisteten Schutz steht.
- Ein zweiter Ansatz könnte darin bestehen, ein Recht auf Schutz eventuell klageweise geltend zu machen. Erforderlich für diesen rechtlichen Ansatz ist, dass sich aus den objektiv-rechtlichen Schutzpflichten zugleich ein subjektives Recht des Betroffenen auf Gewährleistung dieses Schutzes durch den Staat ergibt.

a. Recht auf Selbstschutz

Statt darauf zu vertrauen, dass der Staat seinen Schutzpflichten für das Fernmeldegeheimnis (Art. 10 I GG) auch tatsächlich hinreichend nachkommt, könnte der Grundrechtsberechtigte seine telekommunikative Vertraulichkeit durch eigene, d.h. teilnehmerautonome Maßnahmen schützen:

- Der Einsatz von Verschlüsselungsverfahren zur Gewährleistung der Vertraulichkeit von Kommunikation ist in Deutschland nicht verboten oder in sonstiger Weise beschränkt. Der Einzelne kann somit seine Datenkommunikation selbst schützen.
- Der Einzelne kann durch die Nutzung von Anonymisierungsdiensten auch die Vertraulichkeit seines Informationsverhaltens sicherstellen.

solche nur in Betracht, wenn eine hinreichend konkrete Verpflichtung zum Erlass eines bestimmten Gesetzes bestand; vgl. *v. Danwitz*, in*: v. Mangoldt/Klein/Starck*, GG, Art. 34, Rn. 114. Eine „hinreichend konkrete" Verpflichtung zum Erlass eines bestimmten Gesetzes in diesem Sinne kann jedenfalls nur jenseits des gesetzgeberischen Einschätzungs-, Wertungs- und Gestaltungsspielraums vorliegen – jede andere Sichtweise wäre zutiefst widersprüchlich. Steht dem Gesetzgeber ein Spielraum zu, dann kann die Nutzung dieses Spielraums auch keine Haftung auslösen.

aa) Subsidiarität staatlichen Schutzes?

Zum Teil wird in der Literatur[1428] darauf hingewiesen, dass der staatlich zu gewährleistende Schutz dort ende, wo der Grundrechtsberechtigte sich selbst schützen kann:

> „Der verfassungsrechtlich geforderte Schutz endet da, wo der Betroffene in der Lage ist, die Beeinträchtigung mit eigenen Mitteln abzuwehren bzw. sich ihr zu entziehen."[1429]

Dies würde bedeuten, dass immer dann, wenn der Einzelne sich selbst schützen kann, gar kein staatlicher Schutzpflichtenauftrag mehr bestünde.[1430] Die Gewährleistung staatlichen Schutzes wäre subsidiär und auf die Fälle beschränkt, in denen der Grundrechtsberechtigte sich nicht (wirksam) selbst schützen kann. Für diesen Subsidiaritätsgedanken spricht, dass grundsätzlich auch der schutzbedürftige Grundrechtsberechtigte in seiner Selbstbestimmtheit und Eigenverantwortung[1431] zu achten ist:[1432]

> „Der Rechtsstaat schuldet auch dem schutzbedürftigen Bürger grundrechtliche Distanz. Zur grundrechtlichen Freiheit gehört die Entscheidung des Betroffenen, ob er die staatliche Hilfe in Anspruch nimmt oder die Gefahr riskiert, die Rechtsverletzung aushält, verzeiht, ignoriert, sich nur um die Abwicklung der privatrechtlichen Folgen kümmert."[1433]

Die Grenze der Selbstbestimmtheit und Eigenverantwortung könnte bei der Verletzung öffentlicher (überindividueller) Interessen[1434] oder aus Zumutbarkeitsaspekten[1435] erreicht sein.

Andererseits könnte man staatlichen Schutz und Selbstschutz auch im genau umgekehrten Subsidiaritätsverhältnis zueinander sehen:[1436] Nach der ideengeschichtlichen Herleitung und Begründung von Schutzpflichten verzichtet der Einzelne zu Gunsten des Staates auf die private gewaltsame Durchsetzung seiner Rechte und Interessen. Dieser Verzicht wirkt aber nach *Hobbes* nur, wenn und soweit der Staat

1428 *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 245 f.; *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 142 f.; *Hadamek*, Art. 10 GG und die Privatisierung der Deutschen Bundespost, S. 174 ff.; *Ronellenfitsch,* DuD 2008, 110, 112.

1429 *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 245.

1430 Siehe ausführlich und im Ergebnis ablehnend dazu *Nitz*, Private und öffentliche Sicherheit, S. 382.

1431 Man denke etwa an die eigenverantwortliche Selbstgefährdung, die dementsprechend auch weder verboten ist noch (strafrechtlich) sanktioniert wird. Der Einzelne muss lediglich die Konsequenzen seines Handelns tragen.

1432 Auch *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 245 sowie *Hadamek*, Art. 10 GG und die Privatisierung der Deutschen Bundespost, S. 174 heben die freie Entscheidungsmöglichkeit des Einzelnen hervor.

1433 *Isensee*, Das Grundrecht auf Sicherheit, S. 48 f.

1434 *Isensee*, Das Grundrecht auf Sicherheit, S. 49.

1435 So *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 245; *Hadamek*, Art. 10 GG und die Privatisierung der Deutschen Bundespost, S. 174 und wohl auch *Möstl,* DÖV 1998, 1029, 1036.

1436 So auch die Argumentation von *Nitz*, Private und öffentliche Sicherheit, S. 382.

den Einzelnen im Austausch für dessen Verzicht auf private Gewaltanwendung auch tatsächlich schützt:

> „Die Verpflichtung der Untertanen gegenüber dem Souverän dauere nur so lange, wie er sie auf Grund seiner Macht schützen könne, und nicht länger."[1437]

Danach wäre der private Selbstschutz subsidiär gegenüber der staatlichen Schutzgewährleistung. Zwar steht bei *Hobbes* der Verzicht auf *körperliche* Gewaltausübung im Vordergrund. Seine Ideen zur Legitimation des Staates und zu dessen Aufgaben gelten aber umfassender.[1438] Das staatliche Gewaltmonopol steht hier für die gesamte Rechtsordnung, die durch den Staat gewährleistet und aufrecht erhalten wird – unter anderem auch durch die Ausübung physischer Gewalt. Dabei ist im modernen Staat die tatsächliche Ausübung körperlicher Gewalt sogar die Ausnahme, regelmäßig nimmt der Staat seine Schutzaufgaben auf anderem Weg wahr.

Aus dem soeben Dargelegten ergibt sich, dass staatlicher Schutz und privater Selbstschutz zwar in einem inhaltlichen Zusammenhang stehen, das Verhältnis aber nicht durch einen simplen Vorrang des einen oder des anderen beschrieben werden kann. Staatliche Schutzgewährleistung und privater Selbstschutz stehen vielmehr in einem Verhältnis wechselseitiger Interdependenz:

- Einerseits muss (und soll) der Staat da keinen (aufgedrängten) Schutz gewährleisten, wo der Einzelne sich wirksam selbst schützen kann:

  Kein staatlicher Schutz bei wirksamem Selbstschutz.

- Andererseits ist der Einzelne immer dann zum (auch gewaltsamen) Schutz seiner Rechte und Interessen befugt, wenn der Staat keinen wirksamen Schutz zu gewährleisten vermag:

  Privater Selbstschutz bei unwirksamem staatlichen Schutz.

- Umgekehrt schließt wirksamer staatlicher Schutz die Berechtigung zur eigenmächtigen Selbsthilfe (Selbstjustiz etwa) aus:

  Kein Selbstschutz bei wirksamem staatlichem Schutz.

- Schließlich kann die Stärkung der Selbstschutzmöglichkeiten des Einzelnen (etwa durch staatliche Informations- und Aufklärungsarbeit) selbst ein Mittel zur Erfüllung des staatlichen Schutzpflichtenauftrags sein:[1439]

1437 *Isensee*, Das Grundrecht auf Sicherheit, S. 58.

1438 Und wurden stets auch in diesem umfassenderen Sinn rezipiert (s.o. unter 2.a.cc)).

1439 *Nitz*, Private und öffentliche Sicherheit, S. 391. Dieser nennt außerdem die Verpflichtung des Einzelnen zu Eigensicherungsmaßnahmen als Beispiel für eine Erfüllung staatlicher Schutzpflichten durch Selbstschutzmaßnahmen des Einzelnens. Nach der zustimmungswürdigen Konzeption von *Nitz* beseitigen Selbstschutzmöglichkeiten nicht die staatliche Schutzpflicht,

Staatlicher Schutz durch Selbstschutz.

Privater Selbstschutz und staatlicher Schutz stehen daher wohl mehr in einem wechselseitigen Abhängigkeits-, denn in einem Ausschließlichkeitsverhältnis.[1440] Ob der Schutz bestimmter grundrechtlicher Rechtsgüter eher im Wege des Selbstschutzes oder stärker durch staatliche Schutzmaßnahmen erfolgt, entscheidet zunächst der Gesetzgeber. Ihm kommt auch insoweit ein Einschätzungs-, Wertungs- und Gestaltungsspielraum zu. Wesentliche Kriterien, die im Rahmen dieser Abwägungsentscheidung zu berücksichtigen sind, sind die Wirksamkeit des (staatlich oder selbst geleisteten) Schutzes, die Zumutbarkeit privaten Selbstschutzes sowie die Eigenverantwortung des Grundrechtsberechtigten.

bb) Privates Selbstschutzrecht

Der Einschätzungs-, Wertungs- und Gestaltungsspielraum des Gesetzgebers hat aber auch hier Grenzen. Nach dem Gedanken von *Hobbes* darf der Staat dem Grundrechtsberechtigten Selbstschutzmaßnahmen nicht untersagen, wenn er selbst keinen wirksamen Schutz gewährleisten kann. Dies bedeutet für den Schutz des Fernmeldegeheimnisses durch den teilnehmerautonomen Einsatz von Verschlüsselungsverfahren, dass dieser auch nach der grundrechtlichen Schutzpflichtdimension keinesfalls untersagt werden darf:[1441]

> „Da der einzelne Staat aufgrund der Struktur des Internets nicht gewährleisten kann, daß das Netz hinreichend sicher gestaltet wird, muß er die Bürger durch die freie Zulassung der Verschlüsselung zum Selbstschutz befähigen.“[1442]

Der Staat kann effektiven Schutz der Vertraulichkeit von Fernmeldekommunikation im Internet auf rechtlichem Weg nicht gewährleisten – und wird dies auch in Zukunft nicht können (soweit sich nicht die Informations- und Kommunikationsinfrastruktur selbst grundlegend ändert):[1443] Eine isolierte nationalstaatliche Regulierung muss an der Internationalität der Netzstruktur scheitern.[1444] Eine internationale Regulierung ist nicht absehbar angesichts höchst unterschiedlicher nationaler Interessen und Ressourcen.[1445] Da Daten spurenlos lesbar und veränderbar sind, kann

sondern wandeln diese – wenn der Rechtsgüterschutz durch die Selbstschutzmaßnahmen hinreichend ist – in eine Garantenstellung mit Beobachtungspflichten und Auffangverantwortung um; *Nitz*, Private und öffentliche Sicherheit, S. 379.

1440 *Groß,* JZ 1999, 326, 334 spricht von einem Ergänzungsverhältnis.

1441 So *Groß,* JZ 1999, 326, 334; *Roßnagel,* ZRP 1997, 26, 29; *Trute*, Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57, 216, 259, 263 f.

1442 *Groß,* JZ 1999, 326, 334.

1443 Siehe zum Folgenden auch *Groß,* JZ 1999, 326, 333 f.; *Trute,* JZ 1998, 822, insbes. 263 f.; *Roßnagel,* ZRP 1997, 26, 27 f.

1444 *Brüning/Helios,* Jura 2001, 155, 162.

1445 Sog. *failed states* – um nur ein Beispiel fehlender Regulierungsmöglichkeiten zu nennen – kennen eben keine effektive Ausübung von Hoheitsgewalt.

vermutet werden, dass sich die Strafverfolgung selbst bei Existenz entsprechender Straftatbestände äußerst schwierig gestalten würde.[1446] Ist das (objektive) Entdeckungsrisiko bei Begehung einer Straftat gering, steigert dies die Bereitschaft zur Tatbegehung,[1447] so dass eine Zunahme derartiger Delikte prognostiziert werden kann. Das Internet eröffnet außerdem zusätzliche Möglichkeiten, sich wirksam staatlicher Kontrolle und Strafverfolgung zu entziehen.[1448] Zusammengefasst:

> „In dieser neuen Welt hat der Staat kein Zwangsmittel, kein Gewaltmonopol und keine Souveränität."[1449]

Soweit es um eigene staatliche Informations- und Kommunikationsangebote geht, können staatliche Institutionen die Vertraulichkeit aber auf technischem Weg sicherstellen. Aus den entsprechenden datenschutzrechtlichen Normen ergibt sich in verfassungskonformer Auslegung eine *Pflicht zum Einsatz von Verschlüsselungsverfahren* zur Gewährleistung der Vertraulichkeit. Wird dieser Pflicht – wie festgestellt – vielfach de facto nicht Genüge geleistet, kann der Grundrechtsberechtigte nicht auf diesen unzureichenden staatlichen Schutz verwiesen werden.

> „Technischer Selbstschutz als ein wichtiger Baustein des Schutzes individueller Autonomie wie gesellschaftlichen Informationsaustausches sollte gerade von einem in seiner elementaren Schutzgewährungsfunktion zurückgenommenen Staat solange nicht entwertet werden, wie nicht staatliche Schutzmöglichkeiten ihrerseits angemessen sind."[1450]

Selbst wenn staatliche Schutzmechanismen und privater Selbstschutz *im Ergebnis* gleich wirksam wären, könnten diese Selbstschutzmaßnahmen nicht untersagt werden – da sie in jedem Fall schneller, unkomplizierter und bezüglich des tatsächlichen Erreichens des angestrebten Erfolgs zuverlässiger sind:[1451]

1446 Zumal es bei Kenntnisnahme oder Manipulation nicht-körperlicher Daten mittels einer globalen Netzinfrastruktur keinen Tat*ort* im eigentlichen Sinne mehr gibt.

1447 So hängt nach *Hermann*, Werte und Kriminalität, S. 270 ff. die Rückfallwahrscheinlichkeit von Normakzeptanz und (subjektivem) Entdeckungsrisiko ab.

1448 *Roßnagel,* ZRP 1997, 26, 27.

1449 *Roßnagel,* ZRP 1997, 26, 28.

1450 *Trute*, Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57, 216, 264.

1451 *Hadamek*, Art. 10 GG und die Privatisierung der Deutschen Bundespost, S. 177 f. kommt mit abweichender Begründung zum selben Ergebnis: „Da der Staat nicht lediglich wie vormals in der Abwehrdimension zum Unterlassen von Eingriffen verpflichtet, sondern durch seine Schutzverpflichtung aus Art. 10 GG gebunden ist, aktiv den Schutz dieses Grundrechts zu gewährleisten, ist er umso mehr gehalten, dort Freiraum zu gewähren, wo private Initiative ihm diese Schutzpflicht abnimmt. Der Schutzpflichtenaspekt beeinflußt die Abwägung des privaten Interesses an Datenschutz und Handlungsfreiheit mit den Belangen des Staatsschutzes zugunsten individueller Freiheiten. Denn mit den Schutzpflichten ist eine zusätzliche Begründungsebene in die Grundrechtsdogmatik eingezogen worden, die Aussagen über die Abgrenzung zwischen staatlichen Aufgaben und privater Freiheit beinhaltet. Auch für diese Ebene gilt der Grundsatz der Primärverantwortung des Individuums und dem Vorrang grundrechtlicher Freiheit vor staatlichen Zwecken. Für die Kryptokontroverse bedeutet das, daß die Schutzpflichten aus Art. 10 GG eine liberale Kryptopolitik verlangen."

„Ein solches Selbsthilfeverbot kann selbst einen Freiheitseingriff und einen Verstoß gegen die staatliche Pflicht, Sicherheit zu gewährleisten, darstellen, wenn der Bürger, der seine Rechtsgüter vielleicht selbst besser verteidigen könnte, als es der Staat vermag, `auf die Inanspruchnahme staatlicher Schutzmechanismen verwiesen wird, die wie gerichtlicher Rechtsschutz langwieriger, materiell aufwendiger und unsicherer in Bezug auf den Erfolg sein können als die Selbsthilfe´."[1452]

cc) Selbstschutz trotz staatlichen Schutzes?

Das vom Gesetzgeber im Rahmen seiner Schutzpflichterfüllung zu gewährleitende Schutzniveau ist aber nicht das einer absoluten Sicherheit, eines absoluten Schutzes – die es nicht geben kann. *Für die Schutzpflichterfüllung reicht es mithin aus, wenn grundsätzlich wirksamer Schutz gewährt wird – auch wenn in Einzelfällen tatsächlich kein wirksamer Schutz erfolgt.*

Für das Verhältnis von privatem Selbstschutz und staatlichem Schutz muss allerdings ein anderer Maßstab gelten: Selbstschutz ist unmittelbare Grundrechtswahrnehmung durch den Berechtigten.[1453] Die Untersagung von Selbstschutzmaßnahmen stellt daher stets einen Eingriff in das betreffende Grundrecht dar.[1454] Diesen mit der Erfüllung des staatlichen Schutzauftrages für eben das eingeschränkte Grundrecht rechtfertigen zu wollen wäre anachronistisch. Eine verfassungsrechtliche Rechtfertigung könnte allenfalls zu Gunsten anderer Rechtsgüter gelingen. Für das Fernmeldegeheimnis ist aber oben bereits nachgewiesen worden, dass ein Verbot des Einsatzes von Verschlüsselungsverfahren als Selbstschutzmaßnahme nicht verfassungsrechtlich gerechtfertigt werden kann.

Daher schließt die Gewährleistung von grundsätzlich wirksamem staatlichen Schutz private Selbstschutzmaßnahmen nicht aus. Der Maßstab, wann wirksamer Schutz vorliegt, ist insoweit anders zu beurteilen. *Nur auch im Einzelfall wirksamer staatlicher Schutz führt zu einem Ausschluss privater Selbstschutzmaßnahmen.*

Ein Blick auf die Rechtslage bei privater Gewaltanwendung bestätigt diese Auffassung: Der Einzelne verzichtet auf die Anwendung privater Gewalt zur Durchsetzung seiner Rechte zu Gunsten des staatlichen Gewaltmonopols, soweit und solange der Staat dem Einzelnen dafür wirksamen staatlichen Schutz gewährt. Der Staat schützt zum Beispiel das Leben und die Gesundheit (Art. 2 II S. 1 GG) (unter ande-

1452 *Meyn*, Verschlüsselung und Innere Sicherheit, S. 128 unter Zitierung von *Robbers*, Sicherheit als Menschenrecht, S. 127.

1453 *Hadamek*, Art. 10 GG und die Privatisierung der Deutschen Bundespost, S. 177 vertritt sogar, dass der Staat verpflichtet sei, `dort Freiraum zu gewähren, wo private Initiative ihm diese Schutzpflicht abnimmt´.

1454 Siehe oben in Teil 3. So auch *Grote,* KritV 1999, 27, 53: „Die Frage, ob er dem einzelnen angesichts der beschränkten staatlichen Handlungsmöglichkeiten zur Herstellung von Sicherheit im Netz den Rückgriff auf u.U. wirksamere Selbstschutzmöglichkeiten wie Kryptographie verwehren darf, betrifft dagegen nicht mehr den Inhalt der Schutzpflicht; sondern die mögliche Rechtfertigung eines staatlichen Eingriffs in das zugrundeliegende materielle Grundrecht."

rem) durch entsprechende Straftatbestände (§§ 211 ff., 223 ff. StGB). Damit liegt grundsätzlich ein wirksames Schutzkonzept vor.[1455] Selbst wenn im Einzelfall trotzdem jemand verletzt oder getötet wird, ist das staatliche Schutzkonzept grundsätzlich wirksam.[1456] Allerdings wird bei mangelndem staatlichen Schutz im Einzelfall die private Gewaltanwendung nicht mehr ausgeschlossen: Notwehr als legitime private Gewaltanwendung ist zulässig bei einem gegenwärtigen, rechtswidrigen Angriff im Einzelfall. Der Grundrechtsberechtigte wird also nur auf den Gewaltverzicht verwiesen, solange und soweit er auch im Einzelfall wirksam durch den Staat geschützt wird.

Selbstschutzmaßnahmen dürften demnach nur dann untersagt oder unterbunden werden, wenn der Staat tatsächlich immer wirksamen staatlichen Schutz gewährleistet. Dies ist nach der oben erwähnten Unmöglichkeit absoluter Sicherheit grundsätzlich nie der Fall. Einzige Ausnahme könnten insoweit E-Government- oder E-Justice-Anwendungen sein: Setzt der Staat hier wirksame Maßnahmen zur Gewährleistung der Vertraulichkeit, sprich Verschlüsselung,[1457] ein, muss er nicht noch zusätzlich eine teilnehmerautonome Verschlüsselung unterstützen. Gestalten staatliche Stellen also direkt ein technisches Verfahren, ist es verfassungsrechtlich unbedenklich, wenn dieses zwar teilnehmerautonome Verschlüsselung nicht unterstützt, allerdings selbst wirksamen staatlichen Schutz durch den Einsatz einer Ende-zu-Ende-Verschlüsselung gewährleistet.

dd) Staatlicher Schutz trotz Selbstschutzes?

Da somit dem Einzelnen Selbstschutzmaßnahmen zum Schutz der Vertraulichkeit grundsätzlich offen stehen, könnte die Erforderlichkeit der Gewährleistung staatlichen Schutzes entfallen. Voraussetzung wäre allerdings, dass der Selbstschutz wirksam ist. Dies dürfte kaum jemals derart umfassend gewährleistet sein, dass der Staat keinerlei Schutzmaßnahmen mehr ergreifen müsste:

1455 Davon ausgehend, dass es auch keine gravierenden Durchsetzungsdefizite o.ä. gibt.

1456 So vom Tenor her auch *Ronellenfitsch,* DuD 2008, 110, 112, der zugleich eine Obliegenheit des Einzelnen, sich durch defensive Selbstschutzmaßnahmen angemessen selbst zu schützen, befürwortet.

1457 Erforderlich ist aber die Implementierung einer Ende-zu-Ende-Verschlüsselung und nicht nur einer Leitungsverschlüsselung wie sie etwa das SSL-Protokoll anbietet, da nur so das erforderliche Sicherheitsniveau gewährleistet wird; vgl. Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, M 4.90 Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells, verfügbar unter: http://www.bsi.bund.de/gshb/deutsch/m/m04090.htm (07.01.2009): „Existiert beispielsweise keine Ende-zu-Ende-Verschlüsselung zur Sicherung der Vertraulichkeit einer Kommunikationsbeziehung zwischen zwei Teilnehmern, so liegen die Daten in mindestens einem weiteren Netzelement unverschlüsselt vor." Siehe zur parallelen Kritik der Konferenz der Datenschutzbeauftragten an den geplanten Bürgerportalen Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16.04.2009, verfügbar unter: http://www.sachsen-anhalt.de/LPSA/index.php?id=35083 (20.04.2009).

- Der Großteil der Datenströme im Internet ist nach wie vor unverschlüsselt. Einer Studie des `Instituts für Internet-Sicherheit´ zufolge sollen nur zwischen fünf und 15 Prozent der Daten verschlüsselt sein, wobei die eingesetzten Verfahren in mehr als der Hälfte der Fälle veraltet sind.[1458] Dabei umfassen die genannten Prozentzahlen nicht nur die vom betroffenen Nutzer selbst vorgenommene Ende-zu-Ende-Verschlüsselung von E-Mails, sondern ebenso die durch den Anbieter implementierte Leitungsverschlüsselung, etwa beim Online-Banking oder im Rahmen von Online-Handel.[1459] Der Prozentsatz der tatsächlich vom einzelnen Betroffenen selbst implementierten Ende-zu-Ende-Verschlüsselungsverfahren ist damit noch um einiges niedriger.[1460]
- Dieses mangelnde Interesse an Vertraulichkeitsschutz scheint dabei nur zu einem geringen Teil auf fehlendes Wissen über die Möglichkeiten, dass Daten ausgespäht und E-Mails mitgelesen werden können, zurückzuführen zu sein. Die Tatsache, dass Daten im Internet grundsätzlich in für jedermann lesbarer Form übermittelt werden, ist mittlerweile weithin bekannt. Weshalb dieses Wissen sich nicht verstärkt in Sicherheitsmaßnahmen des Einzelnen niederschlägt, kann nur gemutmaßt werden:
  Zum einen findet sich verbreitet das Argument, die eigenen Daten gingen in den immensen Datenströmen geradezu unter, so dass die Wahrscheinlichkeit, dass ausgerechnet die eigene E-Mail mitgelesen werde, äußerst gering sei. Diese Behauptung wird gestützt mit dem Hinweis darauf, dass die eigene E-Mail-Kommunikation ja völlig belanglos für Dritte sei. Implizit wird also davon ausgegangen, nur die Kommunikation etwa von Prominenten sei von Interesse. Die Möglichkeiten, persönliche Informationen zur Verwirklichung weiterer Angriffe (insbesondere im Wege des `*Social Engineering´*) zu nutzen, werden dabei nicht erkannt.[1461] Dies trägt wahrscheinlich mit dazu bei, dass bei vielen eine gewisse

1458 heise online vom 18.12.2008, Internet-Anwender sind Verschlüsselungsmuffel, verfügbar unter: http://www. heise.de/newsticker/Internet-Anwender-sind-Verschluesselungsmuffel--/meldung/120671 (19.12.2008); *Bär*, Handbuch zur EDV-Beweissicherung, S. 481 nennt für die USA einen Anteil verschlüsselter Kommunikation in der Größenordnung von 10 %.

1459 Nur die Ende-zu-Ende-Verschlüsselung gewährleistet einen umfassenden Schutz vor unbefugter Kenntnisnahme.

1460 Für die Richtigkeit dieses Ergebnisses spricht auch eine vom Zentrum für Europäische Wirtschaftsforschung im Jahr 2005 durchgeführte Unternehmensbefragung (Zentrum für Europäische Wirtschaftsforschung, FAZIT-Kurzbericht: Open Source-Software und IT-Sicherheit, verfügbar unter: http://www.fazit-forschung.de/fileadmin/_fazit-forschung/downloads/Kurzbericht_Nr.1_2005.pdf (17.12.2008), S. 3). Danach nutzen insgesamt nur 29 Prozent der Unternehmen Verschlüsselungsverfahren; sogar im IT-und Mediensektor sind es nur 35 Prozent. Wenn selbst da, wo erstens ein ausgeprägteres Sicherheitsbewusstsein (Betriebs- und Geschäftsgeheimnisse!) herrschen dürfte und zweitens der technische Sachverstand vorhanden ist oder ohne Weiteres eingekauft werden kann, nur ein knappes Drittel Verschlüsselungsverfahren einsetzt, kann davon ausgegangen werden, dass der entsprechende Prozentsatz bei Privatleuten noch erheblich niedriger ist.

1461 Dazu trägt sicher auch bei, dass das Potential der Vernetzung und Auswertung von Daten häufig nur schwer vorstellbar ist. Der Einzelne stellt sich mithin nur vor, die konkrete Information aus einer E-Mail würde Dritten bekannt. Da sicherlich viele E-Mails aus Sicht des Be-

Gleichgültigkeit gegenüber dem Schutz der Vertraulichkeit ihrer Kommunikation festzustellen ist. Es scheint über den Glauben an die Belanglosigkeit der eigenen Kommunikation hinaus aber auch eine Abnahme des Stellenwertes, den Privatheit für den Einzelnen hat, vorzuliegen. Dazu mag beitragen, dass „Privatheit" ebenso wie „Datenschutz" ein äußerst abstraktes Konzept darstellt, soweit es um (zunächst) unbemerkte Privatheitsverluste geht. Sicherlich tragen einerseits Bequemlichkeit, aber andererseits auch das Gefühl mangelnder technischer Kompetenz zu dieser Haltung bei.[1462] Hat der Einzelne das Gefühl, der Informations- und Kommunikationstechnik weitgehend hilflos ausgeliefert zu sein, dürfte allein diese Annahme schon zu einem Weniger an Selbstschutzmaßnahmen führen.

- Der Staat wird daher durch die Existenz von Selbstschutzmöglichkeiten nicht von seiner Schutzpflicht entbunden. Er muss vielmehr – insbesondere, wenn er selbst keinen wirksamen Schutz gewährleisten kann – Selbstschutzmaßnahmen der Grundrechtsberechtigten fördern.[1463] Auch die Förderung von Selbstschutzmöglichkeiten ist staatliche Schutzpflichterfüllung.[1464] Diese Förderung kann zum Beispiel durch staatliche Informationsangebote,[1465] staatliche Förderung entsprechender Forschungsprojekte[1466] oder Schulungsangebote[1467] erfolgen.
  Der staatliche Schutz darf dabei nicht nur aus strafrechtlichen Sanktionsnormen bestehen; es sind in jedem Fall (auch) außerstrafrechtliche Präventivmittel ein-

troffenen belanglos sind, ist dies anscheinend keine besonders erschreckende Vorstellung. Was im Wege der Verknüpfung von Informationen, Profilbildung usw. tatsächlich über den Einzelnen herausgefunden werden kann, liegt häufig außerhalb der Vorstellungskraft des Einzelnen (teils in Unkenntnis der Methoden, teils auf Grund der Abstraktheit der Materie). Vgl. zu den Möglichkeiten der Profilbildung aus Informationen aus `*Social Networks*´, auch wenn diese zum Teil anonym genutzt wurden, sowie anderen Gefährdungen der Privatsphäre in derartigen sozialen Netzwerken Chew/Balfanz/Laurie, (Under)mining Privacy in Social Networks, verfügbar unter: http://w2spconf.com/2008/papers/s3p2.pdf (12.01.2009), S. 2 f.

1462 Dies legen auch die Ergebnisse einer Umfrage nah, in der die Nutzer laut heise online vom 28.01.2009, Datenschützer: US-Regierung soll europäische Datenschutzkonvention unterzeichnen, verfügbar unter: http://www.heise.de/newsticker/Datenschuetzer-US-Regierung-soll-europaeische-Datenschutzkonvention-unterzeichnen--/meldung/122537 (29.01.2009) angaben, zu wenig über rechtliche und technische Schutzinstrumente zu wissen.

1463 *Hadamek*, Art. 10 GG und die Privatisierung der Deutschen Bundespost, S. 178 weist auf die notwendige Zumutbarkeit für den Einzelnen hin, Selbstschutzmaßnahmen zu ergreifen und sieht dies sowohl unter finanziellen als auch unter technischen Gesichtspunkten kritisch.

1464 Ob daneben weitere staatliche Schutzmaßnahmen erforderlich sind, ist eine Frage der Wirksamkeit des staatlichen Schutzkonzepts. In der Regel wird dies aber zu bejahen sein; so ist nicht denkbar, dass die alleinige Förderung von Selbstschutzmaßnahmen den Staat vom Erlass datenschutzrechtlicher Regelungen entbinden könnte.

1465 So gibt es etwa ein Informationsangebot des BSI für Bürger, auch zur Verschlüsselung von Daten; siehe unter http://www.bsi-fuer-burger.de (22.12.2008).

1466 Vgl. etwa das GNU Privacy Projekt (GNUPP), das vom Bundesministerium für Wirtschaft und Arbeit gefördert wurde; siehe unter http://www.gnupp.de (22.12.2008).

1467 Denkbar wäre etwa die Schaffung entsprechender Angebote bei den Volkshochschulen oder die Aufnahme solcher Inhalte in die Lehrpläne der einzelnen Bundesländer.

zusetzen.[1468] Der Einsatz des Strafrechts darf stets nur `*ultima ratio*´ sein – wie auch das BVerfG urteilt:

> „Das Strafrecht ist zwar nicht das primäre Mittel rechtlichen Schutzes, schon wegen seines am stärksten eingreifenden Charakters; seine Verwendung unterliegt daher den Anforderungen der Verhältnismäßigkeit. Aber es wird als "ultima ratio" dieses Schutzes eingesetzt, wenn ein bestimmtes Verhalten über sein Verbotensein hinaus in besonderer Weise sozialschädlich und für das geordnete Zusammenleben der Menschen unerträglich, seine Verhinderung daher besonders dringlich ist.“[1469]

Das BVerfG sieht insoweit klar einen Vorrang präventiver Maßnahmen vor repressiven Maßnahmen.[1470]

- Diese Fördermaßnahmen dienen auch der Vorbeugung eines zusätzlichen `*digital divide*´[1471] auch auf dem Gebiet der Vertraulichkeit von Informations- und Kommunikationsverhalten. Ohne entsprechende staatliche Förderung von Selbstschutzmaßnahmen würde die digitale Gesellschaft einer zunehmenden Spaltung entgegensehen – in eine technologisch versierte Elite, die ihre Kommunikation eigenständig zu schützen in der Lage ist, und den Großteil der Durchschnittsbürger, die dies ohne Hilfestellung nicht können und deren Fernmeldegeheimnis somit schutzlos preisgegeben wäre:[1472]

  > „Der Wandel zur Informationsgesellschaft bedarf allerdings der sozialen und kulturellen Einbettung. Ohne eine ausreichende öffentliche Zugangsinfrastruktur, ohne eine Förderung der Medienkompetenzen der Nutzer, aber auch ohne eine Begrenzung oder Kompensation der Privatisierung und Kommerzialisierung einstmals öffentlicher Informationsbestände, wird die Informationsgesellschaft vorhandene soziale und kulturelle Disparitäten im Umgang mit Informationen verstärken; damit würde der Auftrag zu einem Grundrechtsvoraussetzungsschutz verfehlt.“[1473]

Die Existenz von Selbstschutzoptionen entbindet den Staat somit nicht von seiner Verpflichtung, die Vertraulichkeit der Fernmeldekommunikation zu gewährleisten. Er ist gehalten, Selbstschutzmaßnahmen als derzeit wirksamste Maßnahme zum Schutz des Fernmeldegeheimnisses zu fördern:[1474]

> „Wo staatliche Mittel der Erfüllung von Schutzpflichten angesichts der Weitläufigkeit möglicher Beeinträchtigungsvorgänge, der begrenzten Reichweite staatlicher Regulierungsmöglich-

1468 So auch *Dannecker,* BB 1996, 1285,1291 f. unter Verweis auf internationale Forderungen.
1469 BVerfGE 88, 203, 258 – Schwangerschaftsabbruch II.
1470 Vgl. BVerfGE 39, 1, 44 – Schwangerschaftsabbruch I.
1471 Siehe zu Begriff und Ausprägungen des `*digital divide*´ *Scheule,* InfSpekt 2005, 474.
1472 Insoweit verwirklichen staatliche Maßnahmen, die der digitalen Spaltung der Gesellschaft entgegenwirken sollen, auch das Gleichheitsgebot des Art. 3 I GG, der auch eine soziale Gleichstellung im Sinne von Maßnahmen des sozialen Ausgleichs fordert; *Heun*, in: *Dreier,* GG, Art. 3, Rn. 66; *Starck*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 3, Rn. 33 ff.
1473 *Trute*, Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57, 216, 254.
1474 So auch *Marauhn,* KritV 1999, 57, 75 f.: "Aus verfassungsrechtlicher Perspektive läßt sich sowohl mit Blick auf Art. 10 GG als auch hinsichtlich des Rechts auf informationelle Selbstbestimmung argumentieren, daß es erforderlich ist, diesen privaten Selbstschutz nicht nur zu ermöglichen, sondern auch zu fördern, […]."

keiten und fehlender Kontrollressourcen begrenzt sind, liegt es nahe, privaten Selbstschutz zu ermöglichen und zu fördern."[1475]

Im Wege der Förderung privater Selbstschutzmaßnahmen kommt der Staat zugleich seiner eigenen Schutzpflicht nach.[1476] Angesicht der derzeitigen, umfassenden (Selbst-)Schutzdefizite und des stetigen technischen Fortschritts ist nicht absehbar, dass der Staat auf solche Fördermaßnahmen in Zukunft verzichten können wird. Zum einen besteht ein erheblicher Förderungsbedarf, wie der bisher äußerst spärliche Einsatz von Verschlüsselungsverfahren durch die Nutzer zeigt. Zum anderen werden die technischen Schutzkonzepte angesichts technischer Weiterentwicklung, neuer Angriffsszenarien etc. ebenfalls stetig weiterentwickelt werden müssen, und die Grundrechtsberechtigten in der Adaption veränderter Maßnahmen unterstützt werden müssen. Schließlich wird der Gesetzgeber ohnehin im Rahmen seiner Beobachtungspflicht die technische Entwicklung hinsichtlich der Möglichkeiten zu Selbstschutzmaßnahmen weiterhin im Auge behalten müssen, da nicht abzusehen ist, ob und wie sicher der Einzelne sich in Zukunft selbst schützen können wird:

„Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann. Ein technischer Selbstschutz kann zudem mit einem hohen Aufwand oder mit Funktionseinbußen des geschützten Systems verbunden sein. Viele Selbstschutzmöglichkeiten – etwa die Verschlüsselung oder die Verschleierung sensibler Daten – werden überdies weitgehend wirkungslos, wenn Dritten die Infiltration des Systems, auf dem die Daten abgelegt worden sind, einmal gelungen ist. Schließlich kann angesichts der Geschwindigkeit der informationstechnischen Entwicklung nicht zuverlässig prognostiziert werden, welche Möglichkeiten dem Nutzer in Zukunft verbleiben, sich technisch selbst zu schützen."[1477]

Der Staat bleibt daher im Wege seiner Schutzpflicht verpflichtet, private Selbstschutzmaßnahmen zu fördern, indem er die nötige technische Kompetenz der Grundrechtsberechtigten herstellt und sichert.

Daneben muss der Gesetzgeber aber auch einen rechtlichen Rahmen zur Gewährleistung des Fernmeldegeheimnisses schaffen. Insbesondere da, wo der Staat selbst Angebote im Internet macht (vor allem im E-Government und in der E-Justice, aber auch bei einfachen Kontaktformularen auf den Internetseiten staatlicher Stellen), kann es dem staatlichen Schutzauftrag nicht genügen, dass der Staat Selbstschutzoptionen fördert und die Grundrechtsberechtigten darauf verweist. Für diese Sichtweise spricht auch die „Mitverantwortungs-Rechtsprechung" des BVerfG seit der Mühlheim-Kärlich-Entscheidung.[1478] Schutzpflichten können danach einen (von der

1475 *Trute*, Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57, 216, 263.

1476 Zumindest hinsichtlich dieser Teilmaßnahme wird man von einer kooperativen Schutzpflichterfüllung sprechen können; *Trute*, Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57, 216, 263.

1477 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 180.

1478 BVerfGE 53, 30 – Mühlheim-Kärlich.

Schutzintensität) dem Abwehrrecht angenäherten Schutz auslösen, wenn der Staat eine besondere Mitverantwortung für die Grundrechtsgefährdungen trägt:[1479]

> „Wird aber ein Kernkraftwerk trotz des in ihm verkörperten außerordentlichen Gefährdungspotentials im Allgemeininteresse an der Energieversorgung genehmigt, so bedeutet dies, daß die körperliche Integrität Dritter Gefährdungen ausgesetzt werden kann, die diese nicht beeinflussen und denen sie kaum ausweichen können. Damit übernimmt der Staat seinerseits eine eigene Mitverantwortung für diese Gefährdungen. Demgemäß erscheint es geboten, bei der verfassungsrechtlichen Beurteilung der materiellrechtlichen und verfahrensrechtlichen Vorschriften für die Genehmigung von Kernkraftwerken nicht weniger strenge Maßstäbe anzulegen als bei der Prüfung staatlicher Eingriffsgesetze."[1480]

Begründete im Fall Mühlheim-Kärlich die staatliche Genehmigung des Kernkraftwerks eine besondere staatliche Mitverantwortung für die vom Kernkraftwerk ausgehenden Gefahren, liegt die Verantwortung für die Gestaltung staatlicher E-Government-, E-Justice- und aller staatlichen Internetanwendungen sogar in der *alleinigen Verantwortung* des Staates. Dies rechtfertigt die Anwendung eines strengeren Maßstabs bei der Frage, ob der staatliche Schutz *hinreichend* ist: *Dort, wo der Staat selbst unmittelbar die Vertraulichkeit der Fernmeldekommunikation sicherstellen kann, muss er dies auch tun*. Um dies sicherzustellen, ist von Seiten des Gesetzgebers ein entsprechender rechtlicher (datenschutzrechtlicher o.ä.) Rahmen aufzustellen. Staatliche Behörden trifft dann wiederum die Verpflichtung, sich an diese rechtlichen Vorgaben zu halten und sie adäquat umzusetzen.

Die technische Möglichkeit zum Selbstschutz durch den Einzelnen entbindet den Staat also nicht von einer eigenständigen Erfüllung seiner Schutzpflicht.[1481]

ee) Zusammenfassung

Den Grundrechtsberechtigten steht somit stets ein Recht auf Selbstschutz bezüglich der Vertraulichkeit ihrer Fernmeldekommunikation zu. Gewährt der Staat im Rahmen seiner Schutzpflicht keinen wirksamen Grundrechtsschutz, liegt dies auf der Hand. Das Gesagte gilt aber gleichermaßen, wenn der Staat durchaus grundsätzlich wirksamen Schutz zu gewährleisten vermag. Auch bei grundsätzlich wirksamem staatlichen Schutz bedeutet dies noch lange keinen wirksamen Schutz in jedem Einzelfall. Hier sind weiter Selbstschutzmaßnahmen vonnöten. Daher kann nur ein staatlicher Schutz, der auch in jedem Einzelfall wirksamen Grundrechtsschutz gewährleistet, Selbstschutzmaßnahmen ausschließen. Schon wegen der Unmöglichkeit absoluter Sicherheit kann eine derartige Situation niemals eintreten.

Trotz der Selbstschutzmöglichkeiten wird auch immer zusätzlicher staatlicher Schutz erforderlich sein. Zum einen, um Selbstschutzmaßnahmen zu verbreiten und

1479 So auch *Möstl,* DÖV 1998, 1029, 1036.

1480 BVerfGE 53, 30, 58.

1481 Die Schutzpflichterfüllung mag dann zum Teil in kooperativer Weise erfüllt werden, es muss sich aber um eine eigene staatliche Schutzpflichterfüllung handeln.

zu fördern, zum anderen, da weitere Maßnahmen nötig sind, um ein effektives staatliches Schutzkonzept zu schaffen.

Schließlich ist der Staat bei eigenen E-Justice-, E-Government- oder sonstigen staatlichen Internetangeboten wegen seiner besonderen (Mit-)Verantwortung für eigene Angebote sowie der häufig festzustellenden technischen Unmöglichkeit teilnehmerautonomen Selbstschutzes verpflichtet, die Vertraulichkeit der Fernmeldekommunikation sicherzustellen. Dies wird in der Regel den Einsatz von Verschlüsselungsverfahren bedeuten.

b. Subjektives Recht auf Schutz

Die staatliche Schutzpflicht besteht zunächst objektiv-rechtlich.[1482] Zu prüfen ist, ob auch der einzelne betroffene Grundrechtsträger ein korrespondierendes subjektives Recht auf staatlichen Schutz hat.

aa) Subjektiv-rechtliche Schutzansprüche aus objektiv-rechtlichen Schutzpflichten?

Dass sich aus objektiv-rechtlichen Schutzpflichten auch entsprechende subjektive Rechte auf Schutz ergeben können, ist vom BVerfG seit dem C-Waffen-Beschluss anerkannt:

> „Daß Art. 2 Abs. 2 Satz 1 GG nicht lediglich ein subjektives Abwehrrecht verbürgt, sondern zugleich eine objektivrechtliche Wertentscheidung der Verfassung darstellt, die für alle Bereiche der Rechtsordnung gilt und verfassungsrechtliche Schutzpflichten begründet, ist in ständiger Rechtsprechung beider Senate des Bundesverfassungsgerichts anerkannt. Werden diese Schutzpflichten verletzt, so liegt darin zugleich eine Verletzung des Grundrechts aus Art. 2 Abs. 2 Satz 1 GG, gegen die sich der Betroffene mit Hilfe der Verfassungsbeschwerde zur Wehr setzen kann.“[1483]

Diese Rechtsprechung hat weitreichende Zustimmung in der Literatur erfahren,[1484] wenn auch mit differierenden Begründungen, die wiederum Bedeutung für die Reichweite des subjektiven Rechts im Einzelfall haben: So wird zum Teil darauf abgestellt, dass die Schutzpflichten in den Grundrechten wurzelten und der objektiv-rechtlichen Grundrechtsdimension – ebenso wie dies beim abwehrrechtlichen Gehalt anerkannt sei – „notwendig“[1485] ein subjektiv-rechtlicher Anspruch auf Schutz ent-

1482 *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 90.

1483 BVerfGE 77, 170, 214.

1484 *Isensee*, Das Grundrecht auf Sicherheit, S. 51 f.; *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 24; *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 210; *Wahl/Masing,* JZ 1990, 553, 562; *Groß,* JZ 1999, 326, 331; *Möstl,* DÖV 1998, 1029, 1032; *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, S. 194 ff.; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 58 ff.; *Brüning/Helios,* Jura 2001, 155, 158 ff. m.w.N.

1485 *Calliess*, in: *Merten/Papier,* HGR II, § 44, Rn. 24.

sprechen müsse.[1486] Dieser Auffassung zufolge besteht für jedes Grundrecht, dem eine Schutzpflichtdimension zukommt,[1487] auch ein entsprechendes subjektives Recht auf Schutz.

Andere Stimmen in der Literatur haben hingegen zutreffend darauf hingewiesen, [1488] dass der Schluss auf ein korrespondierendes subjektives Recht für die objektivrechtliche Schutzdimension keineswegs so natürlich und selbstverständlich sei wie zum Teil behauptet. Insbesondere bei der Begründung von Schutzpflichten mit der den Grundrechten innewohnenden objektiv-rechtlichen Wertentscheidung fragt sich, weshalb der Einzelne dies stellvertretend für die Allgemeinheit rechtlich durchsetzen können soll.[1489]

Nimmt man aber stärker in den Blick, dass es bei den grundrechtlichen Schutzpflichten gerade auch um die Gewährleistung *individueller* Rechte geht, dann überzeugt, dass der einzelne Betroffene insoweit seine Rechtsposition auch durchsetzen können muss.[1490] Dem Kriterium der *individuellen Betroffenheit* kommt daher für den Schutzpflichtenbereich besondere Bedeutung zu. Zur Abgrenzung, wann eine hinreichende individuelle Betroffenheit vorliegt, kann insoweit an die Schutznormlehre des BVerwG und des BVerfG angeknüpft werden:[1491]

> „Für die Unterscheidung zwischen geschützter Rechtsposition und bloßem Rechtsreflex kommt es darauf an, ob der betreffende Rechtssatz nicht nur öffentlichen, sondern – zumindest auch – Individualinteressen zu dienen bestimmt ist.“[1492]

Dies vermag auch deshalb zu überzeugen, da es in Einklang mit dem Erfordernis der Geltendmachung eines subjektiv-öffentlichen Rechts im Rahmen der Klagebefugnis (§ 42 II VwGO[1493]) im Verwaltungsprozess bzw. einer eigenen, gegenwärti-

1486 *Isensee*, Das Grundrecht auf Sicherheit, S. 51 spricht vom grundsätzlich „individualistischen, anspruchsfreundlichen Grundzug des Grundgesetzes“ und einer „Vermutung für das subjektiv öffentliche Recht“ (ebenda, S. 52). In der Sache zustimmend auch *Brüning/Helios,* Jura 2001, 155, 158, der eine abstrakte Geltung der Schutzpflichten befürwortet. Schutzpflichten existieren demzufolge auf Grund jeden Risikos. Letztlich ergeben sich keine besonderen Unterschiede zu r hier vertretenen Auffassung, da auch dann wenn man materiellrechtlich stets ein subjektives Recht für gegeben hält, bleibt es doch prozessual bei der hergebrachten Prüfung des Vorliegens eines subjektiv-öffentlichen Rechts bzw. einer eigenen, gegenwärtigen und unmittelbaren Beschwer.

1487 Und damit jedem Grundrecht, da jedem Grundrecht eine Schutzpflichtdimension innewohnt.

1488 *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 208 ff.; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 60.

1489 *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 209 f.

1490 So auch *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 214; *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 111, Rn. 84: *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, S. 195.

1491 *Brüning/Helios,* Jura 2001, 155, 160; *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, S. 143; in der Sache ebenso *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 216 f.

1492 BVerfGE 27, 297, 307.

1493 Je nach Klageart gegebenenfalls in analoger Anwendung.

gen und vor allem unmittelbaren Beschwer bei der Verfassungsbeschwerde[1494] steht.[1495]

Dieser Auffassung folgend besteht ein subjektives Recht des Einzelnen auf Schutz immer dann, wenn er in grundrechtlichen Rechtspositionen betroffen ist, die gerade auch seinem individuellen Schutz dienen (Kriterium der individuellen Betroffenheit). Dies bedeutet, dass für jedes einzelne Grundrecht zu bestimmen ist, ob und inwieweit es individuelle Rechtspositionen oder Kollektivrechtsgüter schützt. Als Paradebeispiele für subjektive Schutzansprüche aus objektiv-rechtlichen Schutzpflichten wurden Situationen fehlender Abwehransprüche gegen den Staat genannt (Kriterium der Substitution fehlender Abwehransprüche):

> „Wenn die spezifischen Freiheitsverbürgungen der einzelnen Grundrechte daher gleichermaßen wirken sollen, stellt ein Schutzanspruch gegen den Staat einen Ausgleich für den obsolet gewordenen (Privatisierung) oder nie existierenden (neue Technologien) Abwehranspruch gegen den Staat und seine Einrichtungen dar."[1496]

bb) Subjektives Recht auf Schutz aus dem Fernmeldegeheimnis

Das Fernmeldegeheimnis (Art. 10 I GG) schützt die Vertraulichkeit der räumlich distanzierten *Individual*kommunikation – und damit klar Individualrechtsgüter.[1497]

Auch der Gedanke der Substitution fehlender Abwehransprüche trifft auf Art. 10 I GG zu: Das Grundrecht des Fernmeldegeheimnisses ist maßgeblich von der Privatisierung des Telekommunikationsbereichs geprägt, mit der Folge, dass klassischerweise gegenüber dem staatlichen Telekommunikationsanbieter bestehende grundrechtliche Abwehransprüche obsolet geworden sind. Hinsichtlich der neuen Informations- und Kommunikationstechnologien bestanden zum Teil noch nie entsprechende Abwehransprüche, da das Bedürfnis danach erst mit dem technologischen Wandel entstanden ist.[1498]

Jeder, der via Telekommunikationstechnik kommuniziert oder sich informiert, hat somit ein subjektives Recht auf Schutz:

1494 Die Verfassungsbeschwerde wäre in Fällen (sowohl echten wie unechten) gesetzgeberischen Unterlassens der korrekte Primärrechtsbehelf, vgl. *Brüning/Helios,* Jura 2001, 155, 157.

1495 Die Verlagerung der Prüfung der individuellen Betroffenheit insoweit ablehnend *Groß,* JZ 1999, 326, 332 sowie *Möstl,* DÖV 1998, 1029, 1033. Dies ist aber eher eine Frage, wie strikt der auf Zulässigkeitsebene angewendete Maßstab ist, und weniger Kritik, die in der Sache durchgreift.

1496 *Brüning/Helios,* Jura 2001, 155, 160.

1497 So auch *Brüning/Helios,* Jura 2001, 155, 160: „Für einen individuellen Schutzanspruch spricht, dass die Abschottung privater oder geschäftlicher Informationen überhaupt nur dem Interesse des einzelnen Geheimnisträgers dient und ein davon unabhängiger öffentlicher Schutzzweck kaum auszumachen ist."

1498 In der Sache ebenso argumentierend *Groß,* JZ 1999, 326, 333; ähnlich auch *Trute,* JZ 1998, 822, 826.

„Da die Gefahren des Missbrauchs bei der Datenübertragung per eMail eine nicht unerhebliche Gefährdung des Kommunikationsgeheimnisses darstellen und aus Art. 10 GG ein Schutzanspruch abgeleitet werden kann, ist jeder Internetnutzer bei jedem einzelnen Versenden einer eMail selbst und aktuell von den unzureichenden Schutzvorschriften betroffen. Wenn die Gegebenheiten des konkreten Falles offenbaren, dass gesetzgeberische oder sonstige staatliche Maßnahmen den Missbrauch der eMail-Kommunikation mindern können, besteht auch eine unmittelbare Beschwer durch das Unterbleiben dieser Maßnahmen."[1499]

cc) Verhältnis von Selbstschutz zu Schutzanspruch

Das Verhältnis von Selbstschutzmöglichkeiten zu staatlich vermitteltem Schutz (und hierzu gehört selbstverständlich auch ein subjektives Recht auf Schutzgewährung) wurde soeben bereits beleuchtet. Das diesbezüglich herausgearbeitete Koexistenzverhältnis wird bei Betrachtung der Beziehung von Klage- zu Selbstschutzmöglichkeiten bestätigt: Eine Klage muss ihrem Klageantrag nach stets auf eine bestimmte staatliche Schutzmaßnahmen zielen. Eine solche Klage wäre regelmäßig zulässig.[1500] Allerdings wird eine Klage auf Grund des weiten gesetzgeberischen Einschätzungs-, Wertungs- und Gestaltungsspielraums kaum jemals begründet sein. Dazu müsste eine Ermessensreduktion auf Null vorliegen, mithin nur eine einzige Maßnahme geeignet, effektiv und angemessen – sprich: verhältnismäßig – sein:

„Die Einwirkung der Grundrechte bzw. der grundrechtlichen Schutzpflichten des Staates auf das schutzgewährende einfache Recht kann die gesetzlichen Grenzen des eingeräumten Ermessensspielraums im Einzelfall dergestalt verengen, daß jede andere Entscheidung als das Eingreifen ermessensfehlerhaft ist (sog. „Ermessensreduktion auf Null")."[1501]

Dies ist im Hinblick auf die Vielfalt der Schutzoptionen allerdings so gut wie nie der Fall.[1502]

„Dem Gesetzgeber wie der vollziehenden Gewalt kommt bei der Erfüllung dieser Schutzpflichten ein weiter Einschätzungs-, Wertungs- und Gestaltungsbereich zu, der auch Raum läßt, etwa konkurrierende öffentliche und private Interessen zu berücksichtigen. Diese weite Gestaltungsfreiheit kann von den Gerichten je nach Eigenart des in Rede stehenden Sachbereichs, den Möglichkeiten, sich ein hinreichend sicheres Urteil zu bilden und der Bedeutung der auf dem Spiele stehenden Rechtsgüter nur in begrenztem Umfang überprüft werden. Der mit einer solchen Schutzpflicht verbundene grundrechtliche Anspruch ist im Blick auf diese Gestaltungsfreiheit nur darauf gerichtet, daß die öffentliche Gewalt Vorkehrungen zum Schutze des Grundrechts trifft, die nicht gänzlich ungeeignet oder völlig unzulänglich sind."[1503]

1499 *Brüning/Helios,* Jura 2001, 155, 161.

1500 Anders könnte dies nur sein, wenn der Kläger nur Selbstschutzmaßnahmen fordert oder wenn er sich erfolgreich durch Verschlüsselung selbst schützt, klageweise aber mehr Informationen und Schulungen durch den Staat durchsetzen will (fehlendes Rechtsschutzbedürfnis).

1501 *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, S. 188.

1502 So auch *Wahl/Masing,* JZ 1990, 553, 559 sowie *Möstl,* DÖV 1998, 1029, 1038. Ausführlich zur Ermessensreduktion auf Null – vor allem für den Bereich des Polizeirechts – *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, S. 188 ff.

1503 BVerfGE 77, 170, 214 f.

Das BVerfG hat mit dem zweiten Abtreibungsurteil[1504] klargestellt, dass „nicht gänzlich ungeeignet oder völlig unzulänglich“ so zu verstehen ist, dass der Gesetzgeber seinen Einschätzungsspielraum „in vertretbarer Weise“[1505] ausgeübt haben muss. Einen Anspruch auf eine konkrete Schutzmaßnahme wird es daher nur höchst ausnahmsweise geben. Eine solche Ausnahme könnte wegen der besonderen staatlichen (Mit-)Verantwortung im Bereich staatlicher E-Government-, E-Justice- oder sonstiger Internetanwendungen gegeben sein.[1506]

Da somit eine Klage selten Aussicht auf Erfolg hat, kann der Einzelne nicht unter Versagung von Selbstschutzmöglichkeiten auf diese (de facto meist ineffektive) Klagemöglichkeit verwiesen werden (s.o.):

> „Die sozialstaatliche Mindestschutzverpflichtung beschreibt das vom Staat geforderte Niveau an Rechtsgütersicherheit, Selbstschutzmöglichkeiten betreffen aber nicht die Frage des `Ob´ staatlicher Schutzverpflichtung, sondern das `Wie´ ihrer Erfüllung. Vermag Selbstschutz das erforderliche Sicherheitsniveau zu gewährleisten, so kann der Staat möglicherweise seine Schutzverpflichtung durch einen Verweis hierauf erfüllen, damit entfällt aber nicht seine allgemeine Schutzverpflichtung, vielmehr wandelt sie sich in eine Garantenstellung, welche dem Staat eine Beobachtungs- und Auffangverantwortung zuweist.“[1507]

Klagemöglichkeit und Selbstschutz stehen dem Grundrechtsberechtigten somit als Handlungsoptionen gleichberechtigt nebeneinander zur Verfügung.

6. Ergebnis

Das Fernmeldegeheimnis (Art. 10 I GG) umfasst neben der abwehrrechtlichen Grundrechtsdimension auch eine objektiv-rechtliche Schutzpflichtdimension, wobei sich die Schutzbereiche entsprechen. Eine staatliche Pflicht zur Schutzgewährleistung aktualisiert sich bei eingetretenen oder drohenden Rechtsgutsverletzungen durch private Dritte. Die Vertraulichkeit der räumlich distanzierten Kommunikation ist bei allen in irgendeiner Form mit dem Internet verbundenen Netzen und informationstechnischen Systemen stets gefährdet.

Das vorhandene staatliche Schutzkonzept zur Erfüllung der Schutzpflicht aus dem Fernmeldegeheimnis ist zwar geeignet, aber nicht effektiv. Der Gesetzgeber ist daher gehalten, seiner diesbezüglichen Nachbesserungspflicht nachzukommen. Der Einzelne kann angesichts des unzureichenden staatlichen Schutzes zum einen Selbstschutzmaßnahmen treffen und zum anderen seinen subjektiv-rechtlichen Schutzanspruch aus dem Fernmeldegeheimnis klageweise geltend machen. Letztlich wird eine Klage auf Implementierung einer ganz bestimmten Schutzmaßnahme re-

1504 BVerfGE 88, 203 – Schwangerschaftsabbruch II.

1505 BVerfGE 88, 203, 262.

1506 Insbesondere dann, wenn die Nutzung dieser Verfahren verpflichtend ist wie etwa bei der nunmehr verpflichtend auf elektronischem Wege einzureichenden Umsatzsteuervoranmeldung; siehe § 18 I UStG.

1507 *Nitz*, Private und öffentliche Sicherheit, S. 379.

gelmäßig am diesbezüglich weiten Einschätzungs-, Wertungs- und Gestaltungsspielraums des Gesetzgebers scheitern. Der objektiven Schutzverpflichtung des Staates steht also kein entsprechender subjektiver, durchsetzbarer Schutzanspruch gegenüber.

Ausnahme sind staatliche Informations- und Kommunikationsangebote, vor allem im E-Justice- und E-Government-Bereich. Diese muss der Staat verfassungskonform ausgestalten – insbesondere, soweit ihre Nutzung verpflichtend ist. Soweit entsprechende einfachgesetzliche Normen vorhanden sind (s.o. unter 4.c.aa) sowie in Teil 1 unter C.II.), wären die jeweils verantwortlichen Stellen richtiger Anspruchsgegner. Aber auch hier müsste ein bestimmter Klageantrag gestellt werden. Es bleibt insofern Frage des Einzelfalls, ob eindeutig zu treffende Maßnahmen festgestellt werden können, der entsprechende Klageantrag damit hinreichend bestimmt formuliert werden und somit eine Klage erfolgreich sein kann.[1508] Hinsichtlich des Einsatzes von Verschlüsselung in allgemein zugänglichen Netzen zum Schutz der Vertraulichkeit der Kommunikation mittels Telekommunikationstechnik ist dies zu bejahen – auch wenn bisher anscheinend kein entsprechendes Rechtsprechungsbeispiel besteht.

II. Staatliche Schutzpflicht aus dem Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 I GG)?

Neben dem Fernmeldegeheimnis (Art. 10 I GG) könnte sich auch aus dem Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 I GG) eine staatliche Schutzpflicht ergeben, die sich in Verschlüsselungspflichten konkretisiert.

1. Schutzpflichtdimension des Grundrechts auf Unverletzlichkeit der Wohnung (Art. 13 I GG)

Auch dem Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 I GG) kommt – wie allen Grundrechten– eine Schutzpflichtdimension zu. Der Schutzbereich entspricht dem der abwehrrechtlichen Grundrechtsdimension: Geschützt ist also die Wohnung als räumliche Privatsphäre sowie alle Vorgänge, die innerhalb dieser räumlichen Privatsphäre stattfinden, und alle Gegenstände, die sich in der Wohnung befinden. Dazu gehören auch Daten, die sich innerhalb dieser räumlichen Privatsphäre befinden; für Telekommunikationsdaten ist allerdings das Fernmeldegeheimnis (Art. 10 I GG) spezieller.

1508 In diesen Konstellationen könnte ausnahmsweise dann auch – bei Vorliegen seiner allgemeinen Voraussetzungen – an einen Staatshaftungsanspruch aus § 839 BGB i.V.m. Art. 34 GG zu denken sein. Besondere Schwierigkeit wird jedenfalls Feststellung, Beweis und Beziffferung des eingetretenen Schadens bereiten.

2. Rechtsgutsbeeinträchtigung durch private Dritte

Die räumliche Privatsphäre wird neben staatlichen Überwachungsmaßnahmen (Lausch- und Spähangriff, Online-Durchsuchung) gerade auch durch Private bedroht: Sobald ein informationstechnisches System über einen Internetzugang verfügt, können auf diesem System vorhandene Daten grundsätzlich von (staatlichen oder privaten) Dritten überwacht und ausgespäht werden.[1509] So können informationstechnische Systeme sowohl gezielt punktuell durchsucht[1510] als auch dauerhaft laufend überwacht[1511] werden. Möglich ist auch die Nutzung von Kameras oder Mikrofonen eines informationstechnischen Systems zur optischen und akustischen Raumüberwachung.[1512] Insbesondere letztere Möglichkeit hat auch das BVerfG – das ansonsten einen hinreichenden Raumbezug bei Infiltration informationstechnischer Systeme verneint[1513] – als Eingriff in Art. 13 I GG gewertet:

> „Ein weiterer Anwendungsfall des Art. 13 Abs. 1 GG ist die Infiltration eines informationstechnischen Systems, das sich in einer Wohnung befindet, um mit Hilfe dessen bestimmte Vorgänge innerhalb der Wohnung zu überwachen, etwa indem die an das System angeschlossenen Peripheriegeräte wie ein Mikrofon oder eine Kamera dazu genutzt werden.“[1514]

Technisch erfolgt die Infiltration in der Regel entweder durch das (unbeabsichtigte) Ausführen von Dateianhängen oder Downloads, die Schadprogramme enthalten, oder die Ausnutzung von Sicherheitslücken. Gegen die Ausnutzung bisher unentdeckter Sicherheitslücken (`*Less-than-zero-day Exploits*´) kann sich auch ein professioneller Anwender nicht schützen. Bei vielen Nutzern ist allerdings noch nicht einmal die Ausnutzung bisher unentdeckter Sicherheitslücken erforderlich, da weder erforderliche Updates regelmäßig vorgenommen noch ein Trojaner- oder Virenbefall erkannt und beseitigt werden.[1515]

1509 *Pohl,* DuD 2007, 684, 687; s.o. in Teil 1, unter B.II.1.b.

1510 Nach bestimmten Dateien, nach Dateinamen, Dateiendungen, bestimmten Eigenschaften, Schlüsselwörtern etc.; Bundesministerium des Innern, Fragenkatalog des Bundesministeriums der Justiz, verfügbar unter: http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (31.10.2007), S. 6. Siehe zum gesamten Thema auch *Hansen/Pfitzmann/Roßnagel,* DRiZ 2007, 225, 225 ff. und Fox, Stellungnahme zur "Online-Durchsuchung", verfügbar unter: http ://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf (30.12.2008), S. 8.

1511 Insbesondere können Klartextdaten vor einer Verschlüsselung bzw. nach einer Entschlüsselung sowie flüchtige Daten wie Passworteingaben erfasst werden; Bundesministerium des Innern, Fragenkatalog des Bundesministeriums der Justiz, verfügbar unter: http://netzpolitik.org /wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (31.10.2007), S. 6.

1512 So Bundesministerium des Innern, Fragenkatalog des Bundesministeriums der Justiz, verfügbar unter: http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (31.10. 2007), S. 15.

1513 Siehe oben in Teil 3 unter A.II.1.b.cc).

1514 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn.. 193.

1515 Die immensen Bot-Netze zeigen es: derartige Imperien aus fremden Rechnern wären kaum denkbar, wenn alle Nutzer bei warnenden Anzeichen (Menge der übertragenen Daten, CPU-Auslastung) sofort adäquate Gegenmaßnahmen ergreifen würden. Allerdings können auch vermeintlich gut gesicherte IT-Systeme häufig von Fachleuten erfolgreich angegriffen wer-

Dies bedeutet zusammengefasst, dass bei Nutzung von informationstechnischen Systemen, die in irgendeiner Form eine Internetanbindung aufweisen, private Daten aus der räumlichen Privatsphäre jederzeit der Gefahr unbefugter Kenntnisnahme ausgesetzt sind. Eine Rechtsgutsbeeinträchtigung durch private Dritte liegt daher vor.

3. Inhalt und Umfang der Schutzpflicht

Zu prüfen ist, welche konkreten Handlungsaufträge sich aus der staatlichen Schutzpflicht aus dem Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 I GG) ergeben.

a. Staatliches Schutzkonzept

Angesichts des weiten Einschätzungs-, Wertungs- und Gestaltungsspielraums des Gesetzgebers bei der Erfüllung von Schutzpflichten kommt es zunächst auf das bestehende staatliche Schutzkonzept an. Genügt dieses den Anforderungen des Untermaßverbots, kann dem Staat kein anderes oder darüber hinausgehendes Schutzkonzept abgefordert werden.

Im Schutzbereich des Grundrechts auf Unverletzlichkeit der Wohnung (Art. 13 I GG) geht es allein um den Schutz von eigenen Daten des Grundrechtsberechtigten, die sich innerhalb seiner räumlichen Privatsphäre befinden. Das Schutzkonzept kann also notwendig nur Schutzgebote oder ähnliche Regelungen umfassen, die sich an den Grundrechtsberechtigten selbst richten, sowie Normen, die ein Eindringen in die räumliche Privatsphäre verbieten. Regelungen, die Anforderungen an den Umgang staatlicher Stellen mit Daten normieren, sind dagegen zum Schutz der räumlichen Privatsphäre regelmäßig nicht erforderlich.[1516]

den; *Pfitzmann,* InfSpekt 2008, 65, 65. Siehe allgemein zu Maßnahmen der Infiltrationsverhinderung sowie –beseitigung Fox, Stellungnahme zur "Online-Durchsuchung", verfügbar unter: http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf (30.12. 2008), S. 10 ff.

1516 Staatliche Stellen kommen natürlich insoweit als Normadressaten in Betracht als sie etwa strafrechtlichen Verboten ebenso unterworfen sind wie jeder andere. Staatliche Stellen sind also nicht in ihrer Funktion als staatliche Stellen Normadressat. Vielmehr sind Behördenmitarbeiter, Amtsträger usw. ebenso Normadressat wie jede andere Person, die der deutschen Jurisdiktionshoheit unterliegt. Teilweise existieren aber Qualifikationstatbestände für Amtsträger; vgl. etwa § 201 III StGB.

aa) Technischer Missbrauchsschutz bei der Online-Durchsuchung

Ausnahme ist die Rechtsgrundlage für die Online-Durchsuchung, die in § 20k II S. 2 BKAG technische Schutzmaßnahmen der Infiltrationssoftware verlangt, um diese „gegen unbefugte Nutzung“ durch Dritte zu sichern.[1517] Jenseits dieser besonderen Konstellation, dass der Staat selbst in die räumliche Privatsphäre eindringt und private Dritte dieses staatliche Vorgehen für ein eigenes Eindringen ausnutzen können, sind allerdings Normen, die sich in diesem Kontext an staatliche Stellen richten, kaum vorstellbar.

bb) Überwachungs- und Ausspähverbote

Als Verbotsnormen existieren zum einen strafrechtliche Verbote hinsichtlich unbefugter Abhörmaßnahmen; vgl. etwa § 201 I Nr. 1 StGB

> „Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt […]“[1518]

sowie insbesondere § 201 II S. 1, Nr. 1 StGB.

> „Ebenso wird bestraft, wer unbefugt das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört […].“[1519]

§ 201a I StGB stellt die entsprechende Vorschrift für Spähangriffe dar:

1517 Daneben etabliert § 20k VII BKAG einen besondere Schutz des Kernbereichs privater Lebensgestaltung – durch ein Beweiserhebungsverbot (S. 1), ein technisches Vorsorgeprinzip (S. 2), ein Durchsichtverfahren (S. 3), ein Beweisverwertungsverbot (S. 5, 1. Alt.) sowie ein Löschungsgebot (S. 5, 2. Alt.).

1518 Tonträger im Sinne der Vorschrift sind alle Gegenstände, die das gesprochene Wort derart fixieren können, dass eine akustische Reproduktion und Wahrnehmung möglich ist. Dabei kommt es nicht darauf an, ob diese Fixierung auf mechanischem, magnetischem, elektromagnetischem oder digitalem Weg erfolgt; *Graf*, in: *Joecks/Miebach,* MüKo StGB, § 201, Rn. 19.

1519 Abhörgerät kann hier nicht nur ein vom Täter zu diesem Zweck installiertes Gerät sein, sondern gerade auch ein bereits in der Wohnung befindlicher Gegenstand, der entsprechend *verwendet* wird; *Graf*, in: *Joecks/Miebach,* MüKo StGB, § 201, Rn. 31. Soweit in der Literatur Uneinigkeit herrscht, ob auch heutzutage übliche Zusatzausstattungen an Telefonen wie Mithöreinrichtungen, Freisprechanlagen u.ä. noch unter den Begriff der Abhöranlage fallen (für das Vorliegen einer Abhöranlage *Lenckner*, in: *Schönke/Schröder,* StGB, § 201, Rn. 19; gegen die Einbeziehung von Mithöreinrichtungen u.ä. *Graf*, in: *Joecks/Miebach,* MüKo StGB, § 201, Rn. 32; *Heuchemer*, in: *v. Heintschel-Heinegg,* Beck OK StGB, § 201, Rn. 11; *Lackner/Kühl,* StGB, § 201, Rn. 5 m.w. N.), trifft dies jedenfalls nicht die hier relevante Konstellation der zweckentfremdeten Verwendung von Mikrofonen, die in informationstechnischen Systemen oder anderen technischen Geräten in der Wohnung integriert sind. Die Verwendung ist zweckentfremdet, da das Abhören nicht anlässlich eines gerade stattfindenden Telefonats geschieht, sondern ein integriertes Mikrofon für einen Lauschangriff auf das in der Wohnung gesprochene Wort unabhängig von einer eigenen Fernmeldekommunikation des Grundrechtsberechtigten aktiviert wird. Dies fällt nach allen Auffassungen unter den Begriff der Abhöranlage.

„Wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft."[1520]

Daneben sind auch das Ausspähen (§ 202a I StGB)

„Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft."[1521]

und Abfangen von Daten (§ 202b StGB)

„Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist."[1522]

sowie das Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c I StGB)

„Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er 1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder 2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft."

mit Strafe bedroht. Diese Straftatbestände schützen zwar nicht nur, aber auch Daten aus der räumlichen Privatsphäre. Schließlich schützt § 303a I StGB – ebenso wie der Qualifikationstatbestand in § 303b StGB[1523] – ebenfalls Daten aus Wohnungen:

„Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft."[1524]

1520 Die Erfassung auch des „Übertragens" von Bildaufnahmen soll nach dem Willen des Gesetzgebers klarstellen, dass „auch Echtzeitübertragungen, z. B. mittels so genannter `WebCams´ oder `SpyCams´ ohne dauernde Speicherung der aufgenommenen Bilder, einbezogen sind."; BT-Drs. 15/2466, S. 5.

1521 Daten sind „gegen unberechtigten Zugang besonders gesichert", wenn irgendwelche Vorkehrungen getroffen wurden, um den Zugriff auszuschließen oder doch wesentlich zu erschweren. Beispiele sind insbesondere systemimmanente Vorkehrungen wie Passwörter, Magnetkarten, biometrische Erkennungsverfahren, Verschlüsselung, Schreib- und Leseberechtigungen; vgl. *Weidemann*, in: *v. Heintschel-Heinegg,* Beck OK StGB, § 202a, Rn. 13; ausführlich *Graf*, in: *Joecks/Miebach,* MüKo StGB, § 202a, Rn. 31 ff; *Lenckner*, in: *Schönke/ Schröder,* StGB, § 202a, Rn. 8; *v. Bonin*, Die Kontrolle digitaler Kommunikationsinhalte, S. 109.

1522 Während die erste Tatbestandalternative des Verschaffens „aus einer nichtöffentlichen Datenübermittlung" regelmäßig unter das spezielle Fernmeldegeheimnis fallen dürfte, ist ein Verschaffen von Daten „aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage" nach der zweiten Tatbestandsalternative gerade auch aus Wohnungen möglich.

1523 Da auch Geschäftsräume „Wohnungen" im Sinne von Art. 13 I GG sein können.

1524 Während die Vertraulichkeit vor allem von §§ 202a und b StGB geschützt wird, stellt § 303a StGB sonstige Beeinträchtigungen der IT-Sicherheit (teilweise) unter Strafe. Die Strafbarkeit des Löschens, Unterdrückens, Unbrauchbarmachens und Verändern von Daten dient dem

cc) Datenschutzgebote

Gebote, seine Daten zu schützen, können sich demgegenüber – soweit es um die räumliche Privatsphäre geht – nur an den Grundrechtsberechtigten selbst richten. Ein derartiges Gebot existiert für private Nutzer grundsätzlich nicht. Das BDSG (auf welches es allein ankommt, da Privatpersonen nicht-öffentliche Stellen darstellen) ist nur anwendbar bei Datenerhebung, –verarbeitung und –nutzung durch nicht-öffentliche Stellen,

> „soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten."[1525]

Der Großteil der Grundrechtsberechtigten wird auf den eigenen Rechnern innerhalb der räumlichen Privatsphäre regelmäßig vor allem eigene personenbezogene Daten verarbeiten und nutzen. Soweit auch personenbezogene Daten anderer Personen verarbeitet und genutzt werden (naheliegend sind etwa Namen, Adressen, Telefonnummern, E-Mail-Adressen, Geburtstage), wird es dabei in der Mehrzahl der Fälle um persönliche oder familiäre Tätigkeit gehen. Keine persönliche oder familiäre Angelegenheit liegt mehr vor bei geschäftsmäßiger, beruflicher oder gewerblicher Nutzung.[1526] All diejenigen Grundrechtsberechtigten, die auf ihren informationstechnischen Systemen innerhalb ihrer räumlichen Privatsphäre auch berufliche Aufgaben erledigen und dabei (wohl unweigerlich) personenbezogene Daten verarbeiten und nutzen, müssen die technisch-organisatorischen Anforderungen nach § 9 S. 1 BDSG i.V.m. der Anlage zu § 9 S. 1 BDSG erfüllen. Alle übrigen Grundrechtsberechtigten, die auf ihren privaten Rechnern innerhalb ihrer Wohnung nur persönliche oder familiäre Angelegenheiten bearbeiten, trifft kein vergleichbares Gebot, ihre Daten zu schützen.

dd) Verschlüsselungspflichten?

Zu prüfen bleibt, inwieweit sich aus den genannten Normen Verschlüsselungspflichten ergeben (können).

Schutz der Integrität der Daten sowie auch der Gewährleistung der Verfügbarkeit. Von besonderer Bedeutung ist dabei das „Verändern" von Daten, da hierunter (je nach Vorgehensweise) auch das Verbreiten von Computerviren fallen kann, die häufig in einem zweiten Angriffsschritt auch die Vertraulichkeit von Daten gefährden (indem sie Passwörter ausspähen u.ä.); *Ernst,* NJW 2003, 3233, 3238; *Wieck-Noodt*, in: *Joecks/Miebach,* MüKo StGB, § 303a, Rn. 15; *Lackner/Kühl,* StGB, § 303a, Rn. 3; *Weidemann*, in: *v. Heintschel-Heinegg,* Beck OK StGB, § 303a, Rn. 13.

1525 § 1 II Nr. 3 BDSG.

1526 *Gola/Schomerus,* BDSG, § 1, Rn. 21.

- Geht es allein um den Schutz eigener Daten in der räumlichen Privatsphäre, können die Grundrechtsberechtigten kaum zu Selbstschutzmaßnahmen durch den Einsatz von Verschlüsselung rechtlich verpflichtet werden.[1527] Denkbare Maßnahmen sind staatliche Informations-[1528] und eventuell Schulungsangebote. Daneben wird die Frage nach zumutbaren Selbstschutzmaßnahmen des Nutzers häufig in zivilrechtlichen Haftungsfragen eine Rolle spielen.[1529] Entscheidend dafür, welche (Selbstschutz-)Obliegenheiten den Nutzer insoweit treffen, ist die Verkehrsauffassung. Mit steigendem Wissen über Gefährdungen der IT-Sicherheit und zunehmender Zumutbarkeit von Schutzmaßnahmen auch für private Nutzer dürfte das vom Nutzer zu gewährleistende Sicherheitsniveau ansteigen.[1530]

  Eine Verschlüsselungsobliegenheit wird es aller Voraussicht nach aber nicht geben. Abgesehen davon, dass die korrekte Implementierung und Nutzung von Verschlüsselungsverfahren auf absehbare Zeit für den Durchschnittsanwender technisch zu komplex und damit nicht zumutbar sein dürfte, ist Verschlüsselung nicht *das* Mittel, um einer Infiltration seines informationstechnischen Systems

1527 Dem entspricht, dass freiwillige Selbstgefährdung grundsätzlich straflos bleibt. Eine andere Frage ist, inwieweit andere Normen selbstgefährdendes Verhalten mittelbar „bestrafen", etwa versicherungsrechtliche Regelungen, die eine Haftung bei Selbstgefährdung ausschließen. Grundsätzlich ist der Einzelne aber frei, sich selbst zu schädigen.

1528 Siehe etwa die umfangreichen Informationen unter http://www.bsi-fuer-buerger.de sowie http ://www.buerger-cert.de, die das BSI im Rahmen seiner gesetzlichen Aufgabenstellung (§ 3 I Nr. 14 BSIG: „[Aufgaben des Bundesamtes] Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es folgende Aufgaben wahr: […] 14. Beratung und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;") anbietet.

1529 Etwa, inwieweit den Nutzer eine Mitschuld oder gar die Hauptverantwortung (vgl. etwa für Datensicherungsmaßnahmen vor einer Computerwartung OLG, Urteil vom 01.12.2003, Az.: 13 U 133/03, MMR 2004, 487 ff.) für einen eingetretenen Schaden trifft, oder auch, welche Sorgfalt der Nutzer anwenden muss, um mit seinem privaten Rechner nicht wiederum zur Schädigung anderer Nutzer beizutragen (durch die Weiterverbreitung von Viren, die Versendung von Spam über Botnets etc.); vgl. dazu *Koch,* NJW 2004, 801, *Libertus,* MMR 2005, 507. Einen umfassenden Überblick über die Verantwortlichkeit der Nutzer gibt Spindler, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, verfügbar unter: https:// www.bsi.bund.de/cae/servlet/contentblob/486890/publicationFile/30666/Gutachten_pdf.pdf;j sessionid=A2EBB4098A4A5164D2E86814BBC18AEC (04.09.2009), S. 112 ff.

1530 Während der BGH in seinem Urteil vom 04.03.2004, Az.:III ZR 96/03 die Notwendigkeit von Schutzvorkehrungen (im entschiedenen Fall vor Dialern) ohne konkrete Verdachtsmomente abgelehnt hat (ebenda, S. 16), mehren sich die Stimmen im Schrifttum, die etwa die Installation und laufende Aktualisierung eines Virenschutzprogramms für zumutbar halten; *Koch,* NJW 2004, 801, 804, *Libertus,* MMR 2005, 507, 509. Das AG Wiesloch verlangte jüngst in seinem Urteil vom 20.06.2008, Az.: 4 C 57/08, Rn. 45 (juris) eine „irgendwie geartete Absicherung des Computers" gegen Schadsoftware. Die Installation einer kostenfreien Antiviren-Software hielt das Gericht (Rn. 49 ff.) für ausreichend. Die Installation einer Firewall wurde allerdings nicht als notwendig angesehen (vgl. Rn. 51). Diese Einschätzung dürfte aber vor allem auf der vom Gericht vorgenommenen Risikoverteilung zwischen Bank und Kunde beim Online-Banking beruhen (ausführlich dazu Rn. 61 ff.).

und nachfolgender Datenausspähung oder Überwachungsmaßnahmen vorzubeugen:

Während zur Sicherung der Vertraulichkeit von Datenkommunikation Verschlüsselung das einzig wirksame Mittel ist, stellt Verschlüsselung beim Schutz vor Infiltration nur eine von vielen denkbaren Maßnahmen dar, die sich zudem meist ergänzen und nicht ausschließen, etwa Anti-Viren-Programme, *`Honeypot´*- Systeme und -Netze, *`Intrusion-Detection´*- und *`Intrusion-Prevention´*-Systeme.[1531] Daneben stellt Verschlüsselung eine weitere Schutzmaßnahme dar, da ein Angreifer eine Entschlüsselung im Hauptspeicher abwarten muss, bis er für ihn verständliche Informationen erhält.[1532] Als absolut geschützt können aber nur so genannte *`stand-alone´*-Systeme angesehen werden, die über keinerlei Internetverbindung verfügen.[1533] Daneben wurde jüngst als private Schutzmaßnahme gegen Online-Durchsuchungen auch vorgeschlagen, alle Internet-Anwendungen nur über eine *`Virtual Machine´* zu realisieren und so quasi ein virtuelles *`stand-alone´*-System zu verwenden. Einfachste und naheliegende Maßnahme wäre zunächst die Installation eines Virenschutzprogramms sowie einer Firewall.[1534] Eine einfache Maßnahme zum Schutz vor unbefugter Nutzung wäre etwa die Vergabe von Passwörtern (wobei die Passwortdatei selbstverständlich verschlüsselt sein sollte, damit die Maßnahme sinnvoll ist).[1535]

Der alleinige Einsatz von Verschlüsselung ist dagegen gerade kein ausreichendes Sicherheitskonzept im Hinblick auf die Verhinderung unbefugter Kenntnisnahme von Daten, die auf einem informationstechnischen System gespeichert sind: Zum einen können sich noch unverschlüsselte Kopien an anderen Stellen des Systems befinden.[1536] Zum anderen dient eine Infiltration und längere Überwachung eines informationstechnischen Systems ja gerade der Überwindung von Verschlüsselung (Stichwort: Online-Durchsuchung), da auf diesem Wege Daten vor ihrer Verschlüsselung bzw. nach ihrer Entschlüsselung gelesen sowie entsprechende Passwörter ausgespäht werden können.[1537] Verschlüsse-

1531 Aufzählung nach Gesellschaft für Informatik e.V., Pressemitteilung vom 30.08.2007, verfügbar unter: http://www.gi-ev.de/aktuelles/meldungsdetails/meldung/167/ (26.05.2008).

1532 Allerdings kopieren Dateisysteme laut Gesellschaft für Informatik e.V., Pressemitteilung vom 30.08.2007, verfügbar unter: http://www.gi-ev.de/aktuelles/meldungsdetails/meldung/167/ (26.05.2008) aus Sicherheits- und Verwaltungsgründen verschlüsselte Daten auch oftmals in unverschlüsselter Form noch an andere Stellen, auf die ein Angreifer dann eventuell zugreifen kann.

1533 Gesellschaft für Informatik e.V., Pressemitteilung vom 30.08.2007, verfügbar unter: http://www.gi-ev.de/akt uelles/meldungsdetails/meldung/167/ (26.05.2008).

1534 Weitere Vorschläge bei Fox, Stellungnahme zur "Online-Durchsuchung", verfügbar unter: htt p://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf (30.12.2008), S. 10 ff.

1535 *Gola/Schomerus,* BDSG, § 9, Rn. 23.

1536 *Pohl,* DuD 2007, 684, 687.

1537 So nennt das Innenministerium die Online-Durchsuchung als „einzig geeignete Maßnahme, um Dateien im Klartext zu erlangen“; Bundesministerium des Innern, Fragenkatalog des

lung erschwert die inhaltliche Kenntnisnahme von Daten zwar erheblich, die Infiltration eines Systems verhindert sie aber nicht. Eine Verschlüsselungspflicht oder –obliegenheit für Private besteht daher nicht.

- Soweit personenbezogene Daten geschäftsmäßig, beruflich oder gewerblich verarbeitet und genutzt werden – der Schutz von Art. 13 I GG gilt auch für Büro- und Geschäftsräume[1538] und ist insoweit seinem Wesen nach (Art. 19 III GG) auch auf juristische Personen anwendbar[1539] –, sind die technisch-organisatorischen Maßnahmen gem. der Anlage zu § 9 S. 1 BDSG zu treffen. Hier gilt allerdings gleichermaßen, dass Verschlüsselung eine unbefugte Kenntnisnahme zwar erschweren mag, diese aber nicht verhindern kann. Andere Sicherheitsmaßnahmen außer Verschlüsselung sind nicht nur einfacher, sondern hinsichtlich des Schutzes der Daten auch effektiver. Da immer nur nach Aufwand und Schutzzweck angemessene Maßnahmen erforderlich sind (§ 9 S. 2 BDSG), scheidet eine Verschlüsselungspflicht oder –obliegenheit zum Systemschutz auch bei geschäftsmäßiger, beruflicher oder gewerblicher Datenverarbeitung grundsätzlich aus.[1540]
- Ob sich aus dem technischen Missbrauchsschutz nach § 20k II S. 2 BKAG eine Verpflichtung zum Einsatz von Verschlüsselungsverfahren ergibt, kann mangels näherer Informationen zur Ausgestaltung nicht beurteilt werden (s.o. in Teil 1 unter C.II.6.).

ee) Zusammenfassung

Verschlüsselung spielt nach dem staatlichen Schutzkonzept zum Schutz von Daten aus der räumlichen Privatsphäre keine Rolle. Vielmehr schützen strafrechtliche Verbotsnormen vor Überwachung und Ausspähung. Soweit Ausspäh- und Überwachungsmaßnahmen vom Staat selbst durchgeführt werden, existieren umfangreiche Sicherungsmaßnahmen auf Verfahrensebene – insbesondere zum Schutz des Kernbereichs privater Lebensgestaltung. Daneben ist ein technischer Missbrauchsschutz zu gewährleisten. Dieser scheint zum Teil auch auf dem Einsatz von Verschlüsselungsverfahren zu basieren, inwieweit dies zwingend ist, verschließt sich aber einer hiesigen Beurteilung.

Bundesministeriums der Justiz, verfügbar unter: http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (31.10.2007), S. 19.

1538 *Hermes*, in: *Dreier,* GG, Art. 13, Rn. 24 m.v.w.N.

1539 *Hermes*, in: *Dreier,* GG, Art. 13, Rn. 20.

1540 Im Hochsicherheitsbereich mag dies wegen der überragenden Bedeutung der zu schützenden Daten im Einzelfall anders sein. Das Geheimschutzhandbuch des BMWA für die Wirtschaft sieht obligatorische Verschlüsselung aber auch nur für die Datenübertragung sowie tragbare Endgeräte vor; Teil II, Ziffer 1.4 der Anlage 4 sowie Teil B der Anlage 59 zu Bundesministerium für Wirtschaft und Arbeit, Handbuch für den Geheimschutz in der Wirtschaft, verfügbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/bmwa-geheimschutzhandbuch,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf (28.06.2007).

Darüber hinaus ist jeder für den Schutz seiner eigenen Daten innerhalb der räumlichen Privatsphäre selbst verantwortlich, ein allgemeines rechtliches Datenschutzgebot existiert nicht. Personenbezogene Daten anderer Personen sind aber nach den Maßstäben von § 9 BDSG zu schützen.

Verschlüsselungspflichten ergeben sich daraus zur Gewährleistung der Unverletzlichkeit der Wohnung allerdings nicht. Vertraulichkeitsschutz bedeutet in diesem Zusammenhang vor allem Schutz vor Infiltration des informationstechnischen Systems sowie Schutz vor Seitenkanalangriffen. Verschlüsselung kann hier eine unbefugte Kenntnisnahme zwar erschweren, aber nicht wirksam verhindern. Dazu ist ein Bündel an Maßnahmen erforderlich, von denen Verschlüsselung eine sein kann – aber auch nur sein *kann*, und keinesfalls als einzige Maßnahme.

b. Ergebnis

Der Schutz der Unverletzlichkeit der Wohnung basiert somit, auch hinsichtlich des Schutzes von Daten aus der räumlichen Privatsphäre, nicht wesentlich auf dem Einsatz von Verschlüsselungsverfahren. Inwieweit das staatliche Schutzkonzept über diesen hier betrachteten Ausschnitt hinaus effektiv ist und ob es ein effektiveres Schutzkonzept als die Beschränkung auf den Erlass strafrechtlicher Verbote gibt, ist nicht Gegenstand dieser Arbeit. Das Fehlen eines allgemeinen Daten(selbst)schutzgebotes (und vor allem entsprechender Fördermaßnahmen) dürfte aber angesichts der *`ultima ratio´*-Rechtsprechung des BVerfG, das bei der Schutzpflichterfüllung einen Vorrang präventiver Maßnahmen vor repressiven Maßnahmen postuliert, kritisch zu beurteilen sein.[1541]

III. Staatliche Schutzpflicht aus dem allgemeinen Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG)?

Auch aus dem allgemeinen Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG), insbesondere in seinen Ausprägungen als Recht auf informationelle Selbstbestimmung und Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, könnten sich staatliche Schutzpflichten ergeben, die den Einsatz von Verschlüsselungsverfahren erfordern.

1541 BVerfGE 39, 1, 44 – Schwangerschaftsabbruch I: „Dabei gilt auch und erst recht für den Schutz des ungeborenen Lebens der Leitgedanke des Vorranges der Prävention vor der Repression. Es ist daher Aufgabe des Staates, in erster Linie sozialpolitische und fürsorgerische Mittel zur Sicherung des werdenden Lebens einzusetzen."

1. Schutzpflichtdimension des allgemeinen Persönlichkeitsrechts

Das allgemeine Persönlichkeitsrecht verfügt ebenfalls über eine Schutzpflichtdimension:[1542]

> „Das allgemeine Persönlichkeitsrecht enthält zudem eine objektive Schutznorm, die auf die Gestaltung der Rechtsordnung und den Schutz vor Beeinträchtigungen Dritter gerichtet ist.“[1543]

Dies gilt auch für die einzelnen Ausprägungen des allgemeinen Persönlichkeitsrechts, etwa das Recht auf informationelle Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[1544]

Geschützt wird zum einen die Vertraulichkeit von Daten. Für personenbezogene Daten ergibt sich dies aus der Ausprägung des Rechts auf informationelle Selbstbestimmung. Da nach Auffassung des BVerfG die Privatsphärenrelevanz eines Datums aber nicht umfassend vorherseh- und objektivierbar ist,[1545] und es daher kein belangloses Datum mehr geben kann, ist dies denkbar weit zu verstehen. Grenze sind Daten mit nur noch punktuellem Bezug zum Grundrechtsträger. Geschützt wird neben der Datenvertraulichkeit auch die Datenintegrität. Dabei dient der Integritätsschutz in der Sache dem Schutz der Vertraulichkeit der Daten. Denn wenn

> „[….] auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.“[1546]

Voraussetzung für den grundrechtlichen Integritätsschutz ist eine berechtigte Privatheitserwartung des Nutzers eines informationstechnischen Systems, die vom BVerfG bei einer Nutzung des Systems „als eigenes“ bejaht wird.

2. Rechtsgutsbeeinträchtigung durch private Dritte

Das Rechtsgut der Vertraulichkeit von privatsphärenrelevanten Daten ist durch eine Vielzahl von Überwachungs- und Abhörmöglichkeiten privater Dritter gefährdet.[1547]

1542 *Robbers*, Sicherheit als Menschenrecht, S. 197 f. sieht den Schutz der Privatsphäre, das Recht am eigenen Bild und am eigenen Wort wegen ihre engen Bezugs zur Menschenwürde sogar als vom expliziten Schutzauftrag des Art. 1 I S. 2 GG erfasst an.

1543 *Trute, JZ* 1998, 822, 825 m.w.N.

1544 So auch *Hornung,* CR 2008, 299, 305 sowie für das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme *Sick,* VBlBW 2009, 85, der aber zugleich betont, dass das BVerfG jedenfalls in der Entscheidung zur Online-Durchsuchung, die allein Gegenstand seiner Betrachtung ist, keine derartige Schutzpflicht anerkannt habe.

1545 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 197 ff. Vgl. insgesamt zum Schutzbereich Teil 3 unter A.III.1.

1546 BVerfG; Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07, Rn. 204.

1547 Vgl. insoweit die Ausführungen zum Fernmeldegeheimnis unter I.3.a.cc) sowie zum Recht auf Unverletzlichkeit der Wohnung unter II.2.

Das daneben geschützte Rechtsgut der Integrität privatsphärenrelevanter Daten unterliegt ebenfalls umfassenden Gefährdungen:

- Daten in unsicheren Umgebungen (etwa allgemein zugänglichen Netzen wie dem Internet) können von jedem interessierten Dritten unterdrückt oder verändert werden.[1548] Die drohenden Gefahren entsprechen insoweit den für das Fernmeldegeheimnis geschilderten Gefahren.
- Daten in sicheren Umgebungen können vor allem nach einer Infiltration des informationstechnischen Systems – sei es der eigene Rechner des Grundrechtsberechtigten oder ein Intranet – gelöscht oder manipuliert werden. Selbst ein professioneller Nutzer kann eine Ausnutzung bislang unbekannter und unveröffentlichter Sicherheitslücken (*`Less-than-zero-day Exploits´*) nicht verhindern. Es bestehen insoweit parallele Gefahren wie für Daten in der räumlichen Privatsphäre (Art. 13 I GG) geschildert.

Zusammenfassend sind privatsphärenbezogene Daten umfassenden Gefahren der unbefugten Kenntnisnahme wie der unbefugten Veränderung durch private Dritte ausgesetzt.

3. Inhalt und Umfang der Schutzpflicht

Zu untersuchen ist, welche Schutzverpflichtungen sich für den Staat aus seiner Schutzpflicht aus dem allgemeinen Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) ergeben.

a. Staatliches Schutzkonzept

Ausgangspunkt ist wiederum das bestehende staatliche Schutzkonzept: Zu diesem gehören – angesichts paralleler Gefahren sowie Schutzbereichsüberschneidungen – auch die Normen, die bereits bei der Darstellung der Schutzkonzepte zur Gewährleistung des Fernmeldegeheimnisses (Art. 10 I GG) und der Unverletzlichkeit der Wohnung (Art. 13 I GG) genannt wurden. Das allgemeine Persönlichkeitsrecht erfordert aber ein umfassenderes Schutzkonzept:

aa) Verschlüsselung zum Schutz der Vertraulichkeit staatlicher Datenübermittlungen

Während der Schutzbereich des Fernmeldegeheimnisses (Art. 10 I GG) in personeller Hinsicht nur die grundrechtsberechtigten Kommunikationsteilnehmer und deren Daten umfasst, hat das allgemeine Persönlichkeitsrecht, und hier vor allem das Recht auf informationelle Selbstbestimmung, einen breiteren Ansatz. Geschützt

1548 S.o. in Teil 1 unter B.II.1.

werden personenbezogene Daten – gleichgültig, wer die Daten erhebt, speichert, verarbeitet, nutzt etc. Damit erfasst der Schutzbereich des allgemeinen Persönlichkeitsrechts vollständig den Umgang des grundrechtsverpflichteten Staats mit personenbezogenen bzw. privatsphärenrelevanten Daten. Dazu gehört auch der staatliche Umgang mit Daten, die in (insbesondere allgemein zugänglichen) Netzen übermittelt werden. Es geht inhaltlich ebenso wie im Rahmen des Fernmeldegeheimnisses um den Vertraulichkeitsschutz bei räumlicher distanzierter (Daten-)Kommunikation, hier allerdings um den Vertraulichkeitsschutz von staatlicher Kommunikation (mit anderen staatlichen Stellen oder mit Dritten[1549]).

Wie beim Schutzkonzept zu Art. 10 I GG existieren auch hier zahlreiche *explizite Verschlüsselungspflichten* – insbesondere bei Nutzung allgemein zugänglicher Netze; vgl. § 488 I S. 2 StPO. Soweit einfachgesetzliche Normen den Schutz der „Vertraulichkeit", den Schutz „gegen unbefugte Kenntnisnahme" etc. vorschreiben, ergeben sich auch hier *implizite Verschlüsselungspflichten*. Verschlüsselung ist schließlich auch eine *technisch-organisatorische Maßnahme* der Weitergabe- (Nr. 4 der Anlage zu § 9 S. 1 BDSG) bzw. Datenverarbeitungskontrolle (§ 10 II S. 2 Nr. 4 HDSG).

bb) Verschlüsselung zum Schutz von Integrität und Datensicherheit

Darüber hinaus verlangen vor allem die Datenschutzgesetze mit ihren Katalogen technisch-organisatorischer Maßnahmen auch den Schutz der Datenintegrität und allgemeiner der Datensicherheit.

Auch jenseits von Datenübermittlungen ist die Sicherheit informationstechnischer Systeme zu gewährleisten, wie das BVerfG mit der Deduktion des Rechts auf Gewährleistung der Vertraulichkeit und *Integrität* informationstechnischer Systeme aus dem allgemeinen Persönlichkeitsrecht deutlich gemacht hat. Die Kataloge der technischen und organisatorischen Maßnahmen bilden insoweit die Ziele der IT-Sicherheit ab. Zum Schutz der Vertraulichkeit und Integrität von Daten können sich daraus Verschlüsselungspflichten ergeben.[1550]

1549 Hier erfasst ist damit nur staatliche Kommunikation mit einem Privaten hinsichtlich für diesen *fremder* Daten – ansonsten wäre das Fernmeldegeheimnis betroffen. Beispiel könnte etwa die hessische Melderegisterauskunft-online sein: Der Staat kommuniziert mit einem privaten Dritten, übermittelt werden aber in der Hauptsache nicht dessen Daten, sondern die im Melderegister enthaltenen Daten eines anderen.

1550 S.o. in Teil 1 unter C.II.7.

b. Geeignetheit

Da das staatliche Schutzkonzept den Schutz von Vertraulichkeit und Integrität privatsphärenrelevanter Daten jedenfalls fördert, ist es als geeignet anzusehen.[1551]

c. Effektivität

Das staatliche Schutzkonzept könnte sich insbesondere im Hinblick auf den Schutz der Vertraulichkeit und Integrität privatsphärenrelevanter Daten(bestände) in informationstechnischen Systemen als ineffektiv darstellen. Das BVerfG hat in seiner Entscheidung zur Online-Durchsuchung neben personenbezogenen Daten vor allem auch auf die Bedeutung von Datenbeständen hingewiesen.[1552] Alle Daten in einem informationstechnischen System[1553] fallen danach in den grundrechtlichen Schutzbereich:

> „Das Schutzbedürfnis des Nutzers eines informationstechnischen Systems beschränkt sich jedoch nicht allein auf Daten, die seiner Privatsphäre zuzuordnen sind. Eine solche Zuordnung hängt zudem häufig von dem Kontext ab, in dem die Daten entstanden sind und in den sie durch Verknüpfung mit anderen Daten gebracht werden. Dem Datum selbst ist vielfach nicht anzusehen, welche Bedeutung es für den Betroffenen hat und welche es durch Einbeziehung in andere Zusammenhänge gewinnen kann. Das hat zur Folge, dass mit der Infiltration des Systems nicht nur zwangsläufig private Daten erfasst werden, sondern der Zugriff auf alle Daten ermöglicht wird, so dass sich ein umfassendes Bild vom Nutzer des Systems ergeben kann.“[1554]

Nach der Rechtsprechung des BVerfG müsste also auch die Vertraulichkeit und Integrität nicht personenbezogener Daten gewährleistet werden, soweit diese in geschützten informationstechnischen Systemen enthalten sind.

Auf der einfachgesetzlichen Ebene erfolgt der staatliche Schutz aber allein durch die allgemeinen Datenschutzgesetze sowie einige bereichsspezifische Regelungen (Anlage zu § 126 I S. 2 Nr. 3 GBO für Grundbuchdaten; Anlage zu § 78a SGB X für Sozialdaten), die einen parallelen datenschutzrechtlichen Fokus aufweisen. Daher beziehen sich alle Normen allein auf den für *personenbezogene* Daten zu gewährleistenden Schutz (vgl. S. 1 der Anlage zu § 9 S. 1 BDSG; § 10 II S. 1 HDSG; 1. Hs. der Anlage zu § 126 I S. 2 Nr. 3 GBO; S. 1 der Anlage zu § 78a SGB X i.V.m. § 67 I S. 1 SGB X). Hinsichtlich des grundrechtlichen Schutzes nicht personenbezogener

1551 Siehe zum Geeignetheitsmaßstab oben in Teil 3 unter A.I.3.c.bb)(9).

1552 BVerfG, Urteil vom 27.02.2008, Az.:1 BvR 370/07 und 595/07, Rn. 200: „Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein.“

1553 Ausnahme sollen Daten in informationstechnischen Systemen sein, die nach der Konstruktion des Systems nur punktuellen Bezug zu einem bestimmten Lebensbereich des Betroffenen haben; vgl. BVerfG, Urteil vom 27.02.2008, Az.:1 BvR 370/07 und 595/07, Rn. 202.

1554 BVerfG, Urteil vom 27.02.2008, Az.:1 BvR 370/07 und 595/07, Rn. 197.

Daten in informationstechnischen Systemen scheint kein entsprechender einfachgesetzlicher Schutz zu existieren.

Allerdings ist der Begriff des personenbezogenen Datums denkbar weit gefasst; vgl. die Definition in § 3 I BDSG:[1555]

> "Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)."

„Angabe" kann dabei jede Information sein.[1556] „Persönliche oder sachliche Verhältnisse" meint umfassend alle Informationen, die etwas über die Bezugsperson aussagen.[1557] Erfasst werden schließlich nicht nur Angaben über *bestimmte* Personen, sondern auch über lediglich *bestimmbare* Personen. Jedenfalls die Bestimmbarkeit dürfte auch bei Daten in informationstechnischen Systemen ohne – bezogen auf die jeweilige Einzelangabe – Personenbezug gegeben sein. Dadurch, dass die Einzelangabe Teil eines ganzen Datenbestands ist (woraus sich nach dem BVerfG gerade die besondere Schutzwürdigkeit ergibt), wird in der Praxis voraussichtlich immer zumindest Personenbeziehbarkeit gegeben sein.[1558] Daten, die für sich allein keinen Personenbezug aufweisen, können im Zusammenspiel mit personenbezogenen Angaben selbst zum personenbezogenen Datum werden: Daten über die Internetnutzung verfügen an sich nicht über einen Personenbezug, in Verknüpfung mit einer IP-Adresse werden aber personenbezogene Daten daraus.[1559] Die Kategorie des „nicht personenbezogenen Datums in informationstechnischen Systemen mit mehr als punktuellem Bezug zum Betroffenen" könnte somit zwar theoretisch denkbar, faktisch aber nicht existent sein.

Gegen die Effektivität des Schutzkonzepts lassen sich im Übrigen dieselben Einwände vorbringen, die auch schon hinsichtlich des Vertraulichkeitsschutzes im Rahmen des Fernmeldegeheimnisses aufgeworfen wurden: Es fehlt an ausdrücklichen gesetzlichen Verschlüsselungspflichten, Datenschutzverstöße werden nur mangelhaft sanktioniert und selbst diese mangelhaften Sanktionen finden kaum Anwendung, da bereits die Kontrolle von Datenschutzmaßnahmen unzureichend ist. Das Schutzkonzept ist demnach nicht hinreichend effektiv.

1555 So mit übereinstimmendem Wortlaut auch § 2 I HDSG sowie § 67 I S. 1 SGB X für Sozialdaten. Die GBO enthält keine eigenständige Definition des personenbezogenen Datums, so dass insoweit auf die Definition der allgemeinen Datenschutzgesetze zurückzugreifen ist.

1556 *Dammann*, in: *Simitis,* BDSG, § 3, Rn. 5.

1557 *Dammann*, in: *Simitis,* BDSG, § 3, Rn. 7.

1558 So dürften in informationstechnischen Systemen wie Laptops, PDAs u.ä. häufig die IP-Adresse (die zutreffenderweise ganz überwiegend als personenbezogenes Datum angesehen wird; vgl. etwa LG Frankenthal, Beschluss vom 21.05.2008, Az.:6 O 156/08; AG Wuppertal, Urteil vom 03.04.2007, Az.: 22 Ds 70 Js 6906/06; AG Berlin, Urteil vom 27.03.2007, Az.:5 C 314/06; AG Darmstadt, Urteil vom 30.06.2005, Az.: 300 C 397/04; *Dammann*, in: *Simitis,* BDSG, § 3, Rn. 35 ff. und 63; *Brunst*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, S. 342 ff. m.v.w.N.), der Name, die E-Mail-Adresse u.ä. enthalten sein.

1559 So auch *Dammann*, in: *Simitis,* BDSG, § 3, Rn. 63.

4. Folgen ineffektiven staatlichen Schutzes

Da der Staat keinen effektiven Schutz des allgemeinen Persönlichkeitsrechts gewährleistet, stehen den Grundrechtsberechtigten grundsätzlich sowohl Selbstschutzoptionen als auch die gerichtliche Durchsetzung ihres subjektiven Rechts auf staatlichen Schutz offen.

a. Selbstschutzmaßnahmen

Gewährleistet der Staat keinen effektiven Schutz, muss den Grundrechtsberechtigten der Einsatz von Selbstschutzmaßnahmen gestattet sein. Bei ineffektiver staatlicher Schutzpflichterfüllung muss der Staat Selbstschutzmaßnahmen nicht nur passiv dulden, sondern diese darüber hinaus auch aktiv fördern, d.h. die rechtlichen und tatsächlichen Voraussetzungen für effektiven Selbstschutz schaffen. Dies gilt gleichermaßen für den Schutz des allgemeinen Persönlichkeitsrechts: [1560]

> "Der Staat ist in der Verantwortung, seinen Bürgerinnen und Bürgern Instrumente zum informationellen Selbstschutz gegen heimliche Ausspähung an die Hand zu geben und ihren ungehinderten Einsatz zu gewährleisten."[1561]

> „Die aus dem allgemeinen Persönlichkeitsrecht folgende Schutzpflicht gebietet den zuständigen staatlichen Stellen vielmehr, die rechtlichen Voraussetzungen eines wirkungsvollen informationellen Selbstschutzes bereitzustellen.“[1562]

Selbstschutzmaßnahmen kommen natürlich nur da in Betracht, wo der Grundrechtsberechtigte den Umgang mit seinen Daten auch tatsächlich selbst in der Hand hat. Dies ist hinsichtlich des Schutzes von Vertraulichkeit und Integrität eigener informationstechnischer Systeme der Fall. Keinen Einfluss haben die Grundrechtsberechtigten hingegen darauf, wie der Staat mit einmal erhobenen Daten umgeht: Die Vertraulichkeit staatlicher Datenübermittlungen, die Integrität und Datensicherheit von personenbezogenen Daten, die der Staat gespeichert hat, können die Grundrechtsberechtigten nicht durch Selbstschutzmaßnahmen beeinflussen. Selbstschutzmaßnahmen sind also generell möglich, aber nur teilweise zum Schutz des allgemeinen Persönlichkeitsrechts tauglich.

b. Schutzanspruch

Das allgemeine Persönlichkeitsrecht gewährleistet die Grundbedingungen persönlicher Lebensentfaltung. Die bisher anerkannten Teilgehalte wie unter anderem das

1560 So auch *Trute,* JZ 1998, 822, 829.
1561 *Dix*, Neue Perspektiven für den Schutz personenbezogener Daten?, in: *Roggan,* Online-Durchsuchungen, S. 71, 75.
1562 BVerfG, Beschluss vom 23.10.2006, Az.: 1 BvR 2027/02, Rn. 33.

Recht am eigenen Wort, das Recht am eigenen Bild und das Recht am eigenen Datum verdeutlichen, dass es dabei jeweils um den Schutz von Individualrechtsgütern geht.[1563] Den objektiv-rechtlichen Grundrechtsgehalten des allgemeinen Persönlichkeitsrechts entspricht also auch ein subjektives Recht des Einzelnen auf Schutz.

Hinsichtlich des Umgangs des Staates oder Dritter mit personenbezogenen Daten der Grundrechtsberechtigten bleibt den derart Betroffenen allein die gerichtliche Geltendmachung ihres subjektiven Rechts auf Schutz. Da die Betroffenen an der Datenverarbeitung nicht selbst beteiligt sind, sondern diese außerhalb ihrer Einflusssphäre stattfindet, sind Selbstschutzmaßnahmen nicht möglich.

Im Hinblick auf die Durchsetzung von Ansprüchen auf Schutz durch die Grundrechtsberechtigten ist zu unterscheiden zwischen staatlichen Schutzmaßnahmen, die durch Dritte bewirkt werden sollen, und staatlichen Schutzmaßnahmen, die *allein* durch staatliche Stellen bewirkt werden sollen:

- Soll der Staat die personenbezogenen Daten der Grundrechtsberechtigten bei der *Erhebung und Verarbeitung durch Dritte* schützen, stehen dem Staat hierzu die bereits angesprochenen Instrumente (Nachbesserung gesetzlicher Regelungen, staatliche Informationstätigkeit, schärfere Kontrollen, härtere Sanktionen bei Verstößen, Förderung von sog. *`privacy enhancing technologies´* etc.) zur Verfügung. Welche Instrumente der Gesetzgeber einsetzt, unterliegt seinem diesbezüglichen, weiten Einschätzungs-, Wertungs- und Gestaltungsspielraum. Nur in dem seltenen Ausnahmefall einer Ermessensreduktion auf Null – *nur eine* konkrete Schutzmaßnahme ist geeignet, effektiv und angemessen – ergibt sich ein gerichtlich durchsetzbarer subjektiver Schutzanspruch des Grundrechtsberechtigten.
- Geht es um den *Umgang des Staates selbst* mit Daten des Einzelnen, besteht hinsichtlich gesetzgeberischer Maßnahmen ebenfalls der weite Einschätzungs-, Wertungs- und Gestaltungsspielraum, der eine gerichtliche Durchsetzung von Schutzansprüchen in der Regel scheitern lässt. Anders bei der staatlichen Anwendung bestehenden (Datenschutz-)Rechts: Die Einhaltung der gesetzlichen Datenschutz- und Datensicherheitsvorschriften (insbesondere der technisch-organisatorischen Anforderungen nach § 10 II HDSG bzw. der Anlage zu § 9 S. 1 BDSG) ist gerichtlich voll überprüfbar.[1564] Dabei sind die einzelnen techni-

1563 So auch *Robbers*, Sicherheit als Menschenrecht, S. 197: „Verhältnismäßig wenig problematisch ist die Frage, ob Art. 2 Abs. 1 GG insoweit ein Recht auf Schutz gewährleistet, als durch ihn das allgemeine Persönlichkeitsrecht, der Persönlichkeitskern geschützt ist. Aufgabe dieses Rechts ist nach der Rechtsprechung des Bundesverfassungsgerichts, im Sinne des obersten Konstitutionsprinzips der 'Würde des Menschen' die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen zu gewährleisten, die sich durch die traditionellen Freiheitsgarantien nicht abschließend erfassen lassen; diese Notwendigkeit besteht namentlich auch im Hinblick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen der menschlichen Persönlichkeit."

1564 Dies wäre natürlich zunächst ein abwehrrechtliches Szenario: Der Staat trifft bestimmt Datenschutz- und Datensicherheitsmaßnahmen und auf die Klage eines Betroffenen hin prüft das Gericht, ob diese Maßnahmen den datenschutzrechtlichen Anforderungen genügen.

schen und organisatorischen Maßnahmen (nach der Anlage zu § 9 S. 1 BDSG bzw. § 10 II HDSG) gesetzlich durch Zielvorgaben, was im Einzelnen zu gewährleisten und zu verhindern ist, konkretisiert. Daraus ergibt sich natürlich auch hier ein gewisser Spielraum, da keine konkreten Maßnahmen im Gesetz verankert sind. Erforderlich im Sinne des Gesetzes sind dabei immer nur solche Maßnahmen, deren Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht (vgl. § 9 S. 2 BDSG). Mit der Einfügung von folgendem Satz 2 in die Anlage zu § 9 S. 1 BDSG könnte allerdings der Rechtfertigungsdruck bei fehlendem Einsatz von Verschlüsselung ansteigen:

„Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren."

Bestimmte Zielvorgaben können ohnehin technisch nur auf *eine* bestimmte Art und Weise bzw. unter Einsatz einer bestimmten Technologie oder Vorgehensweise umgesetzt werden. Hervorragendes Beispiel hierfür ist der Einsatz von Verschlüsselungsverfahren zur Sicherung der Vertraulichkeit in unsicheren Umgebungen (wie dem Internet). Verschlüsselung ist technisch die *einzige* Möglichkeit, Vertraulichkeit in unsicheren Umgebungen zu gewährleisten. Der Aufwand steht angesichts der Betroffenheit grundrechtlich geschützter personenbezogener Daten *immer* in angemessenem Verhältnis zu diesem Schutzzweck. *Eine Klage auf Schutz personenbezogener Daten in unsicheren Umgebungen durch den Einsatz von Verschlüsselungsverfahren wäre daher erfolgreich*.[1565]

Die Gewährleistung der Integrität von Daten kann technisch ebenfalls nur unter Verwendung von Verschlüsselungsverfahren umgesetzt werden: Der Schutz der Datenintegrität in sicheren Umgebungen erfordert zwingend den Einsatz von Verschlüsselungsverfahren, um die Informationen über die im Rahmen der notwendigen Rechteverwaltung vergebenen Berechtigungen sicher zu speichern. Der Schutz der Datenintegrität in unsicheren Umgebungen erfordert den Einsatz von Hashfunktionen, die mit Hilfe eines kryptographischen Schlüssels neben der Integrität auch die Authentizität von Daten belegen. Auch hier ist also zwingend Verschlüsselung zur Verwirklichung der Zielvorgaben einzusetzen. *Eine Klage auf Schutz der Integrität von Daten durch Verschlüsselungsverfahren wäre grundsätzlich ebenfalls erfolgreich*.[1566]

1565 Gleiches gilt – wie oben unter 3.a.aa) dargelegt – für abgeschottete, lokale Netze, allerdings nur für besonders sensible Daten. Nur bei Betroffenheit sensibler Netze steht dieser zusätzliche Aufwand (neben den ohnehin für das lokale Netz getroffenen Sicherheitsmaßnahmen) in angemessenem Verhältnis zum angestrebten Schutzzweck.

1566 Insbesondere hinsichtlich des Integritätsschutzes in unsicheren Umgebungen könnte dies im Einzelfall anders zu bewerten sein. Es kann hier nicht abschließend für alle denkbaren IT-Sicherheitskonzepte bewertet werden, ob der Einsatz von Verschlüsselungsverfahren in jedem Einzelfall die einzige adäquate Maßnahme zum Integritätsschutz darstellen würde. Nur dann kann eine Klage Erfolg haben. Eine endgültige Beurteilung ist nur an Hand des jeweiligen IT-Sicherheitskonzepts möglich.

- Die gilt umso mehr, soweit es sich um Daten handelt, zu deren Preisgabe der Einzelne *verpflichtet* ist bzw. Verfahren (E-Government, E-Justice etc.) verwendet werden, deren Nutzung für den Einzelnen verpflichtend ist.[1567] Könnte im Hinblick auf die Sicherheitsstandards in optionalen E-Government-Angeboten noch argumentiert werden, dass es dem Einzelnen schließlich freistehe, das Angebot und die damit einhergehende Bequemlichkeit, Schnelligkeit etc. zu nutzen oder auch nicht, fehlt es bei verpflichtender Datenpreisgabe und verpflichtender Nutzung bestimmter Verfahren an dieser Freiwilligkeit. *In Fällen mangelnder Freiwilligkeit der Datenherausgabe sind daher erhöhte Anforderungen an staatliche Schutzvorkehrungen zu stellen*, wie das BVerfG in einer jüngeren Entscheidung betonte, in der es allerdings um privatrechtliche Offenbarungspflichten in einem von Kräfteungleichgewicht geprägten Vertragsverhältnis ging:

  „Ist jedoch ersichtlich, dass in einem Vertragsverhältnis ein Partner ein solches Gewicht hat, dass er den Vertragsinhalt faktisch einseitig bestimmen kann, ist es Aufgabe des Rechts, auf die Wahrung der Grundrechtspositionen beider Vertragspartner hinzuwirken, um zu verhindern, dass sich für einen Vertragsteil die Selbstbestimmung in eine Fremdbestimmung verkehrt.“[1568]

  Der Rechtsgedanke der erhöhten Schutzverpflichtung in Situation des Kräfteungleichgewichts (wie es typischerweise im Über-/Unterordnungsverhältnis des Staats gegenüber dem Einzelnen besteht) dürfte jedoch umfassender zu verstehen sein.

Insgesamt kann festgehalten werden, dass die gerichtliche Geltendmachung subjektiver Schutzansprüche regelmäßig erfolglos bleiben wird, wo der Staat den Schutz durch Dritte verbessern soll. Erhebt und verarbeitet aber der Staat selbst Daten, kann jedenfalls der Einsatz von Verschlüsselung zum Schutz der Vertraulichkeit und der Integrität von Daten in der Regel gerichtlich durchgesetzt werden.[1569]

5. Ergebnis

Auch das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG), insbesondere in seinen Ausprägungen als Recht auf informationelle Selbstbestimmung und als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, hat neben der abwehrrechtlichen auch eine Schutzpflichtdimension. Die durch das allgemeine Persönlichkeitsrecht geschützten Daten sind vielfältigen Gefahren der unbefugten Kenntnisnahme wie der unbefugten Verände-

1567 Vgl. exemplarisch die elektronische Umsatzsteuervoranmeldung gem. § 18 I UStG.

1568 BVerfG, Beschluss vom. 23.10.2006, Az.: 1 BvR 2027/02, Rn. 35.

1569 Bei fehlendem Einsatz von Verschlüsselung ist auch an einen Staatshaftungsanspruch aus § 839 BGB i.V.m. Art. 34 GG zu denken, da eine Amtspflicht zu fehlerfreier Ermessensausübung besteht (vgl. *v. Danwitz*, in: *v. Mangoldt/Klein/Starck*, GG, Art. 34, Rn, 56 ff, ins. 77). Häufig dürfte ein Schaden aber nicht eingetreten oder nur schwer nachweisbar sein.

rung durch private Dritte ausgesetzt. Zwar existiert nach dem staatlichen Schutzkonzept ein Kanon gesetzlicher Normen, die zum Teil ausdrücklich, zum Teil im Wege der (verfassungskonformen) Auslegung den Einsatz von Verschlüsselung zum Schutz der Vertraulichkeit und Integrität von Daten fordern. Verstöße gegen diese Normen werden aber nicht effektiv kontrolliert und in der Praxis kaum sanktioniert. Der staatliche Schutz ist daher nicht hinreichend effektiv.

Die Grundrechtsberechtigten haben daher das Recht, ihr allgemeines Persönlichkeitsrecht selbst durch eigene Schutzmaßnahmen zu schützen. Dies ist praktisch aber nur da möglich, wo die Grundrechtsberechtigten irgendeinen tatsächlichen Einfluss auf den Umgang mit ihren Daten haben. Dies ist bei Daten in der Hand von Dritten und Daten in der Hand des Staates gerade nicht der Fall.

Die Grundrechtsberechtigten haben daneben auch ein subjektives Recht auf Schutz aus dem allgemeinen Persönlichkeitsrecht, da dieses Individualrechtsgüter schützt. Soweit der Staat Schutzmaßnahmen hinsichtlich des Umgangs Dritter mit Daten treffen soll, hat er hierbei einen so weiten Einschätzungs-, Wertungs- und Gestaltungsspielraum, dass die gerichtliche Geltendmachung eines subjektiven Schutzanspruchs kaum jemals erfolgreich sein wird. Soweit staatliche Stellen selbst Daten des Einzelnen erheben oder verarbeiten, sind sie aber aus spezialgesetzlichen Regelungen oder aus den technisch-organisatorischen Anforderungen der allgemeinen Datenschutzgesetze regelmäßig verpflichtet, Verschlüsselungsverfahren zum Schutz der Vertraulichkeit wie der Integrität einzusetzen. Diese konkreten subjektiven Schutzansprüche können regelmäßig auch erfolgreich gerichtlich durchgesetzt werden.

B. Verschlüsselung und wirtschaftliche Betätigungsfreiheit

Stand in der bisherigen Betrachtung zu staatlichen Schutzpflichten vor allem der Schutz privater Geheimnisse und privatsphärenbezogener Daten im Vordergrund, rückt im Rahmen der Grundrechte, die die wirtschaftliche Betätigungsfreiheit gewährleisten, der Schutz beruflicher und betrieblicher Geheimnisse in den Vordergrund. Verschlüsselung dient dabei im Wesentlichen zwei Zwecken:

- Zum einen werden Verschlüsselungsverfahren zum Schutz von Betriebs- und Geschäftsgeheimnissen eingesetzt.[1570]

1570 Darüber hinaus können Verschlüsselungsverfahren auch selbst Betriebs- und Geschäftsgeheimnisse darstellen bzw. durch Art. 14 I GG geschützte Immaterialgüterrechte (originärer Schutz; s.o. in Teil 3 unter B.I.1.a. und b.aa)). Soweit Verschlüsselungsverfahren selbst das zu schützende Geheimnis darstellen, ergeben sich keine gegenüber der Abwehrperspektive abweichenden Gesichtspunkte. Es ist darüber hinaus nicht ersichtlich, dass der Schutz von Verschlüsselungsverfahren als zu schützendes Immaterialgüterrecht oder Geschäftsgeheimnis eines anderen Schutzes bedürfte als jedes sonstige denkbare Recht oder Geheimnis. Ein staatliches Schutzkonzept besteht insoweit (vgl. nur das Rechtsgebiet des gewerblichen Rechtsschutzes oder § 17 UWG). Es ist nicht ersichtlich, dass dieses Schutzkonzept unzureichend und nachbesserungsbedürftig ist. Ausgespart bleibt hier auch das Recht am eingerichteten und

- Zum anderen dient Verschlüsselung dem Schutz von Berufsgeheimnissen.

Insbesondere hinsichtlich der Berufsgeheimnisse ergeben sich häufig Überschneidungen mit dem Privatsphärenschutz. Denn die Informationen, die etwa der Mandant seinem Anwalt oder der Patient seinem Arzt anvertraut, sind regelmäßig personenbezogene Daten und damit auch über Art. 2 I GG i.V.m. Art. 1 I GG geschützt. Ein Telefonat zwischen einem Berufsgeheimnisträger und seinem Klienten unterfällt wie jedes andere Telefonat dem Fernmeldegeheimnis (Art. 10 I GG). Daneben existieren aber auch eigenständige Anwendungsbereiche: Betriebs- und Geschäftsgeheimnisse dürften zum Beispiel eher selten personenbezogene Angaben enthalten; jedenfalls besteht das Schutzinteresse an diesen Informationen nicht deswegen, weil sie (unter Umständen) personenbezogen sind, sondern weil es sich um das Wissenskapital eines Unternehmens handelt.[1571]

I. Juristische Personen als Grundrechtsträger

Unterschiede zwischen Privatsphären- und wirtschaftlicher Perspektive können vor allem hinsichtlich der jeweils Grundrechtsberechtigten bestehen: So steht der grundrechtliche Privatsphärenschutz juristischen Personen grundsätzlich nicht offen,[1572] da es an der wesensmäßigen Anwendbarkeit dieser Grundrechte auf juristische Personen (Art. 19 III GG) fehlt.[1573] Insoweit ist zu differenzieren:

1. Schutz juristischer Personen durch das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art.1 I GG)?

Insbesondere das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) wird regelmäßig als nicht auf juristische Personen anwendbar angesehen[1574] im Hin-

ausgeübten Gewerbebetrieb von Herstellern und Anbietern von Verschlüsselungsprodukten (vgl. dazu oben in Teil 3 unter B.I.1.c.) Auch hier ist ein besonderer Schutzbedarf von Gewerbebetrieben, die sich der Herstellung und dem Vertrieb an Verschlüsselungsprodukten widmen, nicht ersichtlich.

1571 So auch *Kintzi,* DRiZ 2007, 244, 247 f.

1572 A.A. *Isensee*, in: *Isensee/Kirchhof,* HStR V, § 118, Rn. 60, der das Privatheitsbedürfnis juristischer Personen mit der Notwendigkeit von Vertraulichkeit für interne Willensprozesse begründet, dann aber auf das Redaktionsgeheimnis als Berufsgeheimnis verweist.

1573 In der Regel wird es dabei hier um juristische Personen des Privatrechts gehen und nicht um juristische Personen des öffentlichen Rechts. Die weitergehende Fragestellung, inwiefern juristische Personen des öffentlichen Rechts, die wegen ihrer Zugehörigkeit zum staatlichen Bereich eigentlich zunächst auf der Seite der Grundrechtsverpflichteten vermutet werden, auch Grundrechtsberechtigte sein können, soll daher hier nicht erörtert werden. Vgl. zu diesem Themenkomplex ausführlich *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 251 ff. sowie *Dreier*, in: *Dreier,* GG, Art. 19 III, Rn. 55 ff.

1574 *Dreier*, in: *Dreier,* GG, Art. 19 III, Rn. 37.

blick auf den besonderen Menschenwürdebezug dieses Grundrechts.[1575] Jedenfalls soweit es bei den hier näher beleuchteten Teilgehalten im Kern um den Schutz eines privaten Rückzugsbereichs und weniger um den Schutz der persönlichen Selbstdarstellung in der Öffentlichkeit geht, ist dies überzeugend:[1576]

> „Juristische Personen des Privatrechts existieren um ihrer Aufgabe willen und besitzen ihrem Wesen nach keine Privatsphäre."[1577]

Aber auch, wenn man den Grundrechtsschutz juristischer Personen weniger mit der Vergleichbarkeit der grundrechtstypischen Gefährdungslage, sondern eher mit dem vorgelagerten Schutz der hinter einer juristischen Person stehenden natürlichen Personen begründet sieht, ergibt sich keine abweichende Beurteilung. Nach dieser sog. „Durchgriffsthese" [1578] des BVerfG rechtfertigt sich die Erstreckung des Grundrechtsschutzes auf juristische Personen nur,

> „[…] wenn ihre Bildung und Betätigung Ausdruck der freien Entfaltung der natürlichen Personen sind, besonders wenn der "Durchgriff" auf die hinter den juristischen Personen stehenden Menschen dies als sinnvoll oder erforderlich erscheinen läßt."[1579]

- Im Zusammenhang mit dem *Schutz unternehmerischer Betriebs- und Geschäftsgeheimnisse* ergeben sich regelmäßig keinerlei Berührungspunkte mit dem Schutz der Privatsphäre natürlicher Personen.[1580] Daher besteht auch kein Anlass, zum mittelbaren Schutz natürlicher Personen die Grundrechtsgeltung auch auf juristische Personen zu erstrecken.
- Im Kontext von *Berufsgeheimnissen* geht es regelmäßig um Informationen mit Personen- und Privatsphärenbezug, etwa Gesundheitsinformationen bei der ärztlichen Schweigepflicht, höchstpersönliche Erlebnisse (die von den Betroffenen zudem als Verfehlung begriffen werden) beim Beichtgeheimnis, private Informationen aller Art im anwaltlichen Vertrauensverhältnis zu seinem Mandanten.

1575 Siehe *Dreier*, in: *Dreier,* GG, Art. 19 III, Rn. 35 m.w.N. sowie *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 316.

1576 Vgl. die Differenzierung nach den jeweils betroffenen Teilgehalten bei *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 319 und *Böckenförde*, Die Ermittlung im Netz, S. 173 ff. sowie die Nachweise zur Rechtsprechung des BVerfG bei *Dreier*, in: *Dreier,* GG, Art. 2 I, Rn. 82, die ähnliche Tendenzen erkennen lassen. Schließlich hat auch das BVerfG für einzelne Teilgehalte des allgemeinen Persönlichkeitsrechts die Anwendbarkeit auf juristische Personen anerkannt, so etwa hinsichtlich des Rechts am gesprochenen Wort; vgl. BVerfG, Beschluss vom 09.10.2002, Az.:1 BvR 1611/96 und 805/98, Rn. 35. Dabei betont das BVerfG aber zugleich (ebenda, Rn. 32), dass das Recht am gesprochenen Wort nicht mit dem Schutz der Privatsphäre identisch sei. Für das Recht auf informationelle Selbstbestimmung hat jüngst das Niedersächsische OVG in seinem Beschluss vom 15.05.2009, Az.: 10 ME 385/08, verfügbar unter http://www.dbovg.niedersachsen.de/Entscheidung.asp?Ind=05000200800038510 +ME (21.10.2009) entschieden, dass es auch auf juristische Personen anwendbar sei.

1577 *Schmitt Glaeser*, in: *Isensee/Kirchhof,* HStR VI, § 129, Rn. 87.

1578 Vgl. m.w.N. *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 216.

1579 BVerfGE 21, 362, 369; ebenso *Dreier*, in: *Dreier,* GG, Art. 19 III, Rn. 31.

1580 Für diese Bewertung spricht auch § 67 I SGB X, der einerseits Sozialdaten (als personenbezogene Daten natürlicher Personen) und andererseits Betriebs- und Geschäftsgeheimnisse, deren Träger auch juristische Personen sein können, definiert.

Für den Patienten, Gläubigen, Mandanten etc. als Grundrechtsträger unterfallen diese Informationen daher dem allgemeinen Persönlichkeitsrecht und werden durch dieses geschützt. Für den Berufsgeheimnisträger als Grundrechtsberechtigten (sei es eine natürliche Person wie der Rechtsanwalt, der Arzt, der Priester usw. oder eine juristische Person wie etwa eine Rechtsanwaltsgesellschaft (GbR, Partnerschaftsgesellschaft o.a.) oder ein Zeitungsverlag) werden die Informationen aber nicht wegen ihrer Privatsphärenrelevanz geschützt, sondern im Hinblick auf ihre Implikationen für die Berufsausübung. So hat das BVerfG etwa für die Vertraulichkeit der Pressearbeit betont, dass diese Vertraulichkeitsgewährleistung unverzichtbare Voraussetzung für eine funktionierende journalistische Tätigkeit überhaupt ist:

„Dieser Schutz ist unentbehrlich, weil die Presse auf private Mitteilungen nicht verzichten kann, diese Informationsquelle aber nur dann ergiebig fließt, wenn sich der Informant grundsätzlich auf die Wahrung des Redaktionsgeheimnisses verlassen kann."[1581]

Auch jenseits der Grundrechtserstreckung auf juristische Personen geht es beim Schutz von Berufsgeheimnissen also nicht um Privatsphärenschutz, sondern um die Gewährleistung der Voraussetzungen einer effektiven Berufsausübung. Bereits natürliche Personen werden in ihrer Rolle als Berufsgeheimnisträger mithin nicht durch das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art.1 I GG) geschützt.[1582] Für eine Grundrechtserstreckung auf juristische Personen ist somit kein Raum.

Das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) ist daher nicht wesensmäßig auf juristische Personen anwendbar. Juristische Personen sind insoweit nicht grundrechtsberechtigt.

2. Schutz juristischer Personen durch das Fernmeldegeheimnis (Art. 10 I GG)

Anders ist dies hinsichtlich des Fernmeldegeheimnisses (Art. 10 I GG) zu beurteilen. Dieses gewährt zwar auch (speziellen) Privatsphärenschutz, knüpft aber sachlich nicht an den Kommunikationsinhalt, sondern an das Kommunikationsmittel an. Den Vertraulichkeitsgefährdungen der räumlich distanzierten Kommunikation unterliegt dabei jede Information – sei sie privates oder berufliches Geheimnis. Juristische Personen befinden sich mithin in derselben Gefährdungslage wie natürlich Personen auch:

„Auch juristische Personen bedienen sich des Übertragungsmediums der Telekommunikationsanlage und befinden sich deshalb ebenso wie natürliche Personen in einer grundrechtstypischen Gefährdungslage. Außerdem knüpft der Schutz des Fernmeldegeheimnisses, wie oben

1581 BVerfG, Urteil vom 27.02.2007, Az.:1 BvR 538/06 und 2045/06, Rn. 42 – Cicero.

1582 Eine ähnliche Einschätzung zeichnet sich auch bei *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 319 ab, der den Schutz des Namens, der Reputation und der Geschäftsdaten eines Unternehmens zwar durchaus auch dem Schutz des allgemeinen Persönlichkeitsrechts zuordnen will – aber nur soweit diese nicht ohnehin durch Art. 12 oder 14 GG geschützt sind.

ausgeführt wurde, an die Verwendung eines bestimmten Übertragungsmediums an und erfordert keinen auf eine besondere persönliche Sphäre bezogenen Kommunikationsinhalt."[1583]

Schließlich sind beim Schutz von Kommunikation der Schutz natürlicher Personen und juristischer Personen in besonderem Maße verquickt: Denn bei der Kommunikation einer juristischen Personen ist nach der Natur der Sache stets eine natürliche Personen involviert. Mithin dient der Schutz juristischer Personen durch das Fernmeldegeheimnis auch dem vorgezogenen Schutz der dahinter stehenden natürlichen Personen.[1584] Auch nach der „Durchgriffsthese" ist somit die wesensmäßige Anwendbarkeit des Fernmeldegeheimnisses auf juristische Personen zu bejahen.[1585]

3. Schutz juristischer Personen durch das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 I GG)

Das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 I GG) ist zum Teil wesensmäßig auf juristische Personen anwendbar: Soweit der Schutz von Art. 13 I GG auch für Geschäftsräume gilt,[1586] erstreckt sich der Grundrechtsschutz nach der Rechtsprechung des BVerfG auch auf juristische Personen:[1587]

„Zwar ist die Unverletzlichkeit der Wohnung ihrem Ursprung nach ein echtes Individualrecht, das dem Einzelnen im Hinblick auf seine Menschenwürde und im Interesse seiner freien Entfaltung einen "elementaren Lebensraum" gewährleisten soll. Indessen ist für die Beantwortung der Frage, ob ein Grundrecht "seinem Wesen nach" auf juristische Personen anwendbar ist, weniger auf den historischen Ursprung des Grundrechts als vielmehr darauf abzustellen, ob es nur individuell oder auch korporativ betätigt werden kann. Danach genießen grundsätzlich auch Kommanditgesellschaften den Schutz des Grundrechts aus Art 13 Abs. 1 GG; denn diese können – ebenso wie Einzelpersonen – berechtigterweise Inhaberinnen von Wohnungen sein."[1588]

Treffender dürfte hier jedoch die Durchgriffsthese sein: Der Grundrechtsschutz für Geschäftsräume wird auf juristische Personen erstreckt, weil dort natürliche Personen arbeiten. Das BVerfG hat immer wieder betont, dass die ungestörte Berufsarbeit zum Bereich der individuellen Persönlichkeitsentfaltung gehört.[1589] Trotz des Persönlichkeitsbezugs[1590] ist das Grundrecht auf Unverletzlichkeit der Wohnung

1583 BVerfG, Beschluss vom 09.10.2002, Az.:1 BvR 1611/96 und 805/98, Rn. 38.
1584 Vgl. zum Gedanken der „vorgezogenen Verteidigungslinie" *Huber*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 19, Rn. 228.
1585 So auch mit vielen weiteren Nachweisen *Gusy*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 10, Rn. 47; *Hermes*, in: *Dreier,* GG, Art. 10, Rn. 26.
1586 Vgl. dazu BVerfGE 32, 54, 69 ff.
1587 *Gornig*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 13, Rn. 36 ff.
1588 BVerfGE 42, 212, 219.
1589 *Hermes*, in: *Dreier,* GG, Art. 13, Rn. 24 m.w.N.; *Wieland*, in: *Dreier,* GG, Art. 12, Rn. 34; *Gornig*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 13, Rn. 22.
1590 Vgl. auch die diesbezügliche Kritik bei *Hermes*, in: *Dreier,* GG, Art. 13, Rn. 20.

auch auf Betriebs- und Geschäftsräume juristischer Personen anwendbar. Materiell ist der Schutz von Räumen, die nicht dem Wohnen dienen, allerdings schwächer.[1591]

4. Zusammenfassung

Der durch die Privatsphärengrundrechte vermittelte Schutz wird im Ergebnis nur teilweise auf juristische Personen erstreckt: Das Fernmeldegeheimnis (Art. 10 I GG) gilt auch für juristische Personen. Ähnliches gilt hinsichtlich Geschäftsräumen auch für das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 I GG); dieses gewährleistet für juristische Personen aber nur einen materiell abgeschwächten Schutz. Das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) ist nur hinsichtlich mancher Teilgehalte auf juristische Personen wesensmäßig anwendbar. Da diese Teilgehalte hier jedoch nicht in Rede stehen, wird diese Grundrechtserstreckung auf juristische Personen nicht weiter ausgeführt.

Berufsgeheimnisse sowie Betriebs- und Geschäftsgeheimnisse sind daher nach den Privatsphärengrundrechten nur zum Teil geschützt:

- Die Vertraulichkeit der Kommunikation wird durch das Fernmeldegeheimnis (Art. 10 I GG) gleichermaßen für Betriebs- und Geschäfts- wie Berufsgeheimnisse geschützt. Ein weitergehender Grundrechtsschutz ist nicht erforderlich.
- Auch ein räumlicher Geheimnisschutz wird für juristische Personen durch das Grundrecht auf Unverletzlichkeit der Wohnung (Art.13 I GG) gewährleistet. Da es vor allem um den Schutz vor Überwachung und Ausspähung geht, spielt der teilweise abgeschwächte materielle Schutz für Geschäftsräume, der vor allem der Durchsetzung behördlicher Kontrollbefugnisse dient,[1592] insoweit keine Rolle.
- Jenseits dieser Vertraulichkeitssphären gewährleisten die Privatsphärengrundrechte aber keinen Schutz von Berufs-, Betriebs- und Geschäftsgeheimnissen juristischer Personen. Selbst da, wo inhaltlich starke Überschneidungen bestehen (Berufsgeheimnisse bestehen regelmäßig in personenbezogenen und privaten Informationen), differieren Grundrechtsberechtigte und Schutzrichtung.

II. Staatlicher Schutz beruflicher und betrieblicher Geheimnisse?

Berufsgeheimnisse und Betriebs- und Geschäftsgeheimnisse – sowohl von natürlichen wie auch von juristischen Personen[1593] – werden durch die Berufsfreiheit (Art.

1591 Einzelheiten bei *Hermes*, in: *Dreier,* GG, Art. 13, Rn. 25, 114.

1592 Insoweit wird die Schranke des Art.13 VII GG abweichend ausgelegt; vgl. zu den Kriterien der Rechtsprechung *Hermes*, in: *Dreier,* GG, Art. 13, Rn. 114.

1593 *Wieland*, in: *Dreier,* GG, Art. 12, Rn. 70; *Manssen*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 12, Rn. 266; *Wieland*, in: *Dreier,* GG, Art. 14, Rn. 68; *Depenheuer*, in: *v. Mangoldt/Klein/Starck,* GG, Art. 14, Rn. 186.

12 I GG) bzw. die Eigentumsfreiheit (Art. 14 I S. 1 GG) geschützt. Seinen daraus resultierenden grundrechtlichen Schutzpflichten[1594] kommt der Staat im Wege eines staatlichen Schutzkonzepts nach:

- Dieses schützt Berufsgeheimnisse und Betriebs- und Geschäftsgeheimnisse vor unbefugter Preisgabe, etwa *strafrechtlich* durch § 17 I, II UWG sowie § 203 II StGB für Betriebs- und Geschäftsgeheimnisse und §§ 203, 204 StGB für Berufsgeheimnisse.
- Für Berufsgeheimnisträger finden sich zudem häufig *standesrechtliche* Vertraulichkeitsregelungen, etwa in § 43a II BRAO:

  „Der Rechtsanwalt ist zur Verschwiegenheit verpflichtet. Diese Pflicht bezieht sich auf alles, was ihm in Ausübung seines Berufes bekanntgeworden ist. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen."

- Das allgemeine *Datenschutzrecht* richtet sich dagegen allein auf den Schutz personenbezogener Daten (vgl. § 1 II BDSG; § 1 I HDSG). Auf das Auseinanderfallen von Personenbezug und wirtschaftlichem Geheimhaltungsbedürfnis – insbesondere für Betriebs- und Geschäftsgeheimnisse – wurde bereits hingewiesen. Allgemeine Regelungen der Anforderungen an Datenschutz und Datensicherheit jenseits personenbezogener Daten existieren somit nicht.

1. Verschlüsselung zum Schutz von Berufsgeheimnissen?

Da Berufsgeheimnisse in den meisten Fällen personenbezogene Daten umfassen, gelten in der Regel die Datenschutzanforderungen des BDSG,[1595] insbesondere der Anforderungskatalog zur technischen und organisatorischen Sicherheit nach der Anlage zu § 9 S. 1 BDSG.[1596] Zu prüfen ist, ob sich jenseits der gesetzlichen Anforderungen zum Umgang mit personenbezogenen Daten auch besondere Schutzanforderungen für alle Berufsgeheimnisse ergeben, unabhängig davon, ob es sich im Einzelfall um personenbezogene Daten handelt oder nicht. Einfachgesetzliche Grundlage für solche Verschlüsselungspflichten könnten die standesrechtlichen Verschwiegenheitsverpflichtungen (von Ärzten,[1597] Notaren,[1598] Rechtsanwälten, Pfarrern[1599] etc.[1600]) sein.

1594 Zum Vorhandensein einer dem abwehrrechtlichen Gehalt korrespondierenden Schutzpflicht im Schutzbereich aller Freiheitsgrundrechte s.o. unter A.I.2.b.dd).

1595 Da es bei den Berufsgeheimnissen in der Regel um das Verhältnis des Berufsgeheimnisträgers zu seinem Klienten geht, sind keine öffentlichen, sondern nur private Stellen involviert. Anwendbar ist daher das BDSG, vgl. § 1 II Nr. 3 BDSG.

1596 *Kintzi,* DRiZ 2007, 244, 248 sieht dagegen nur „partielle Überschneidungen" der Rechtskreise Datenschutz und Geheimnisschutz: „Nicht alle Daten sind Geheimnisse im Sinne des § 203 StGB, nicht alle Geheimnisse sind Daten im Sinne des Bundesdatenschutzgesetzes."

1597 Etwa § 9 Berufsordnung für die Ärztinnen und Ärzte in Hessen vom 2. September 1998 (HÄBl. 10/1998, S. I - VIII).

1598 § 18 BNotO.

Zu untersuchen ist also, ob sich aus den standesrechtlichen Verschwiegenheitsverpflichtungen eine Pflicht zur Gewährleistung von Vertraulichkeit sowie von Systemintegrität und Datensicherheit ergibt. Je nachdem, ob eine derartige Pflicht zu Datensicherheitsmaßnehmen besteht oder nicht, hat dies Auswirkungen darauf, ob im Unterlassen dieser Maßnahmen ein strafbares „Offenbaren" im Sinne von § 203 StGB zu sehen ist.[1601]

a. Verschlüsselungspflicht bei Datenübermittlungen, insbesondere E-Mails?

Diese Frage, die vor allem hinsichtlich der anwaltlichen wie der notariellen Verschwiegenheitspflicht diskutiert wird, ist in der Literatur umstritten:

Teilweise wird eine Verpflichtung von Berufsgeheimnisträgern zu aktiven Maßnahmen der Vertraulichkeitssicherung abgelehnt.[1602] Diskutiert wird insoweit vor allem, ob eine Verschlüsselungspflicht für E-Mails besteht. Die ablehnenden Stimmen gründen ihre Ablehnung im Wesentlichen auf folgende Argumente:

- Jedenfalls Rechtsanwälte (wobei die Grundsätze auf andere Berufsgeheimnisträger übertragbar sein dürften; d. Verf.) seien nicht zu aktiven vorsorglichen Schutzmaßnahmen verpflichtet. Auch im Übrigen gebe es keine Pflicht, etwa seine Kanzlei durch Sicherheitsschlösser oder Alarmanlagen zu schützen oder Unterlagen in Tresoren zu verwahren.[1603]
- Der E-Mail-Verkehr sei bei genauer Betrachtung gar nicht unsicherer als etwa ein Telefongespräch, eine Faxübermittlung oder auch eine gängige Versendung

1599 Siehe neben dem Beichtgeheimnis (Can. 983 § 1 CIC) etwa die Verpflichtung zur Amtsverschwiegenheit (§ 18 Kirchengesetz über die Dienstverhältnisse der Pfarrerinnen und Pfarrer (Pfarrdienstgesetz) für die Evangelische Kirche in Hessen und Nassau vom 26.11.2003 (ABl. 2004 S. 69)), die in ähnlicher Weise auch in den anderen Pfarrdienstgesetzen besteht.

1600 Vgl. den Katalog von Berufsgeheimnisträgern in § 203 StGB. Einen ausführlichen Überblick über die an verschiedene Berufsgeheimnisträger gestellten standesrechtlichen Anforderungen bietet Spindler, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, verfügbar unter: https://www.bsi.bund.de/cae/servlet/contentblob/486890/publicationFile/30666/Gutachten_pdf.pdf;jsessionid=A2EBB4098A4A5164D2E86814BBC18AEC (04.09.2009), S. 251 ff.

1601 Wobei natürlich zum einen in besonderer Weise dem Bestimmtheitsgebot nach Art. 103 II GG Rechnung zu tragen ist, zum anderen Vorsatz erforderlich ist (für eine Verletzung der berufsrechtlichen Verschwiegenheitspflicht jedoch Fahrlässigkeit ausreicht; vgl. *Lindloff*, E-Mail-Kommunikation von Rechtsanwälten mit Mandanten und Gerichten, S. 90).

1602 So etwa *Degen,* NJW 2008, 1473, 1479; *Härting,* MDR 2001, 61, 62; *Lindloff*, E-Mail-Kommunikation von Rechtsanwälten mit Mandanten und Gerichten, S. 105; Spindler, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, verfügbar unter: https://www.bsi.bund.de/cae/servlet/contentblob/486890/publicationFile/30666/Gutachten_pdf.pdf;jsessionid=A2EBB4098A4A5164D2E86814BBC18AEC (04.09.2009), S. 252 f. m.w.N.

1603 *Härting,* MDR 2001, 61, 62; *Lindloff*, E-Mail-Kommunikation von Rechtsanwälten mit Mandanten und Gerichten, S. 105 f.

mit der Post. Da die genannten Beispiele nie angezweifelte, gängige Praxis seien, könne für den E-Mail-Verkehr kein anderer Maßstab gelten.[1604]

Andere in der Literatur vertretene Auffassungen leiten dagegen aus der anwaltlichen Verschwiegenheitsverpflichtung eine Verschlüsselungspflicht für E-Mails ab.[1605] Diesen Meinungen zufolge lassen sich durchaus auch positive Handlungsverpflichtungen aus Schweigepflichten ableiten. Dem ist zuzustimmen. Es macht aus Sicht des Mandanten im Ergebnis keinen Unterschied, ob vertrauliche Informationen aktiv verraten worden sind oder ob sie Unbefugten zur Kenntnis gelangen konnten, weil der Berufsgeheimnisträger Unterlagen verloren, im Zug vergessen oder in der Öffentlichkeit zugänglichen Räumen hat herumliegen lassen. So ist in der Literatur zu § 203 StGB durchaus anerkannt, dass ein strafbares Offenbaren von Privatgeheimnissen natürlich auch durch Unterlassen erfolgen kann (wenn der Täter eine entsprechende Garantenstellung innehat und das Unterlassen positivem Tun entspricht).[1606] Die Garantenstellung wird wegen der Sonderrolle als Berufsgeheimnisträger regelmäßig zu bejahen sein:[1607]

> "Durch § 203 StGB oder § 17 UWG wird den dort genannten Berufsgruppen aufgrund ihrer besonderen Vertrauensstellung eine gesetzliche Garantenpflicht für die ihnen anvertrauten Informationen und Daten auferlegt."[1608]

Dementsprechend erkennen auch die meisten Vertreter der erstgenannten Auffassung an, dass jedenfalls bei außergewöhnlicher Bedeutung eines Mandats eine Verschlüsselungspflicht besteht:[1609]

> „Aus der Bedeutung des Mandats kann sich ergeben, dass sich die Vertraulichkeitspflichten des Rechtsanwalts verschärfen."[1610]

Verkannt wird dabei nur, dass die besondere Gefährdung von Informationen, die via E-Mail übermittelt werden, gerade nicht die Ausnahme (für besonders sensible

1604 *Härting,* MDR 2001, 61, 61 f.; *Lindloff*, E-Mail-Kommunikation von Rechtsanwälten mit Mandanten und Gerichten, S. 91 ff.

1605 So etwa *Klett/Lee,* CR 2008, 644, 647 mit vielen weiteren Nachweisen; *Backu,* ITRB 2003, 251, 252, *Wagner/Lerch,* NJW-CoR 1996, 380, 383; *Miedbrodt*, in: *Roßnagel,* Handbuch Datenschutzrecht, Kap. 4.9, Rn. 40; für Notare *Benesch,* JurPC 24/2002, Rn. 3 sowie für alle Berufsgeheimnisträger *Knopp/Wilke/Hornung/Laue,* MMR 2008, 723, 725. Zur Annahme einer Verschlüsselungspflicht tendierend auch *Kuner*, in: *Hoeren/Sieber,* Handbuch Multimedia-Recht, Teil 17, Rn. 56 f.

1606 *Cierniak*, in: *Joecks/Miebach,* MüKo StGB, 203, Rn. 52; *Lackner/Kühl,* StGB, § 203, Rn. 17.

1607 *Cierniak*, in: *Joecks/Miebach,* MüKo StGB, 203, Rn. 52.

1608 *Speichert*, Praxis des IT-Rechts, S. 243.

1609 So *Lindloff*, E-Mail-Kommunikation von Rechtsanwälten mit Mandanten und Gerichten, S. 106, der diese aber aus der Vertraulichkeitsverpflichtung aus dem Mandatsvertrag ableitet. Der Mandatsvertrag beinhalte eine vertragliche Nebenpflicht zur Vertraulichkeit, die entsprechend den Umständen des Mandats auszulegen sei. Im Übrigen solle sich die vertragliche Vertraulichkeitsverpflichtung aber mit der gesetzlichen decken. Diese Doppelung der Vertraulichkeitsverpflichtungen vermag nicht zu überzeugen (da sie vollkommen überflüssig ist). Bereits die berufsrechtliche Vertraulichkeitsverpflichtung beurteilt sich nach den tatsächlichen Umständen.

1610 *Lindloff*, E-Mail-Kommunikation von Rechtsanwälten mit Mandanten und Gerichten, S. 106.

Inhalte) darstellt, sondern die Regel – im Hinblick auf die besonderen Vertraulichkeitsgefahren der Datenübermittlung über Internet.[1611]

Es herrscht im Wesentlichen also Einigkeit darüber, dass Berufsgeheimnisträger im Einzelfall zu vorsorgenden Sicherheitsmaßnahmen verpflichtet sein können – jeweils abhängig von der Vertraulichkeitsbedeutung der konkreten Informationen und den Offenbarungsgefahren, die bei objektiver Betrachtungsweise drohen.[1612] Auf diese Weise wird einerseits den Vertraulichkeitsinteressen von Klienten und Mandanten Rechnung getragen, andererseits aber von den Berufsgeheimnisträgern auch keine nicht zu leistende ständige und umfassende Vorsorge hinsichtlich aller denkbaren Gefahren verlangt.

Abweichungen in der konkreten Bewertung, ob eine generelle Verschlüsselungspflicht für E-Mails besteht, gründen auf abweichenden Risikoabschätzungen.[1613] Insoweit ist den eine Verschlüsselungspflicht ablehnenden Stimmen deutlich zu widersprechen:

- Die Vertraulichkeitsgefahren bei Versendung einer E-Mail sind nicht mit denen eines Fax´, eines Telefonats oder eines Briefs zu vergleichen: Im Gegensatz zu hergebrachten Kommunikationsformen ist das Abfangen und Mitlesen von E-Mails für potentielle Täter deutlich einfacher und hinsichtlich des Entdeckungs- und Strafverfolgungsrisikos weniger gefährlich: Der Täter kann sich an beinahe jedem Ort der Welt aufhalten (da körperliche Anwesenheit für diese Angriffe keine Rolle spielt), was unbestreitbar den Täterkreis maßgeblich erweitert. Der Täter kann dabei seine Identität besser verschleiern als dies in der körperlichen Welt möglich wäre. Das Entdeckungsrisiko des Täters sinkt dadurch nicht nur – er weiß in vielen Fällen von vornherein, dass er keinerlei Strafverfolgung zu befürchten hat (da entweder schon eine Ermittlung seiner Identität sowie eine entsprechende Beweissicherung durch ausländische Behörden scheitert oder jedenfalls eine Auslieferung des Täters nicht erfolgt[1614]). Der strafrechtliche Schutz

1611 *Wagner/Lerch,* NJW-CoR 1996, 380, 383 f. Spindler, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, verfügbar unter: https://www.bsi.bund.de/cae/servlet/contentblob/486890/publicationFile/30666/Gutachten_pdf.pdf;jsessionid=A2EBB4098A4A5164D2E86814BBC18AEC (04.09.2009), S. 252 argumentiert etwa, dass die E-Mail-Accounts ja durch Passwörter geschützt seien.

1612 So auch *Lindloff*, E-Mail-Kommunikation von Rechtsanwälten mit Mandanten und Gerichten, S. 106: „Vielmehr verlangt § 43a BRAO nur einen angemessenen Aufwand zur Verhinderung fremder Kenntnisnahme." *Degen,* NJW 2008, 1473, 1479 sieht zwar keine Pflicht zur Verschlüsselung, rät bei erhöhtem Vertraulichkeitsrisiko aber doch dazu.

1613 *Lindloff*, E-Mail-Kommunikation von Rechtsanwälten mit Mandanten und Gerichten, S. 92. So lehnt Spindler, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, verfügbar unter: https://www.bsi.bund.de/cae/servlet/contentblob/486890/publicationFile/30666/Gutachten_pdf.pdf;jsessionid=A2EBB4098A4A5164D2E86814BBC18AEC (04.09.2009), S. 253 zwar eine generelle Verschlüsselungspflicht ab, bejaht eine solche aber bei Verwendung drahtloser Übermittlungsformen (WLAN).

1614 Es gilt insoweit allgemein der Grundsatz, dass eine Auslieferung nur dann erfolgt, wenn die Tat auch im ausliefernden Staat strafbar wäre; vgl. beispielhaft § 3 I Gesetz über die internationale Rechtshilfe in Strafsachen vom 27.06.1994 (BGBl. I, 1537): „Die Auslieferung ist nur zulässig, wenn die Tat auch nach deutschem Recht eine rechtswidrige Tat ist, die den Tatbe-

der Vertraulichkeit von E-Mail-Kommunikation[1615] kann daher nicht in vergleichbarer Weise wie bei brieflicher oder telefonischer Kommunikation als ausreichendes Instrument des Vertraulichkeitsschutzes genannt werden.

- Zum zweiten wird die Bedeutung von Informationen im Zuge der fortschreitenden Digitalisierung unzutreffend eingeschätzt: Angesichts der zunehmenden Quantität digitaler Informationen, deren Permanenz und Verkettbarkeit, den verbesserten Auswertungsmöglichkeiten sowie der Ubiquität von Datenverarbeitungsprozessen, die auch im Hinblick auf zunehmende Miniaturisierung für den Einzelnen immer weniger wahrnehmbar werden, kann nicht (mehr) zwischen wichtigen und belanglosen Informationen unterschieden werden. Die teilweise in der Literatur errichtete Trennlinie von besonders sensiblen bzw. vertraulichen Informationen oder Mandatsverhältnissen existiert so in Wirklichkeit nicht.[1616] Im Einklang mit der hellsichtigen verfassungsgerichtlichen Rechtsprechung gibt es eben kein belangloses Datum mehr. Dies ist zwingend bei der Auslegung der einfachgesetzlichen Verschwiegenheitspflichten zu berücksichtigen. Eine fixe Trennlinie kann es nicht geben, es kann nur im Einzelfall differenziert werden, welche Schutzmaßnahmen angesichts welcher betroffenen Daten erforderlich und angemessen sind.[1617] Für Datenübermittlungen in unsicheren Umgebungen, insbesondere via Internet, wurde bereits gezeigt, dass kein Datum so bedeutungslos ist, dass es angesichts der besonderen Vertraulichkeitsgefährdungen in unsicheren Umgebungen angemessen sein kann, eine E-Mail unverschlüsselt zu versenden.

  „Insbesondere sind Personen in Garantenstellung auch verpflichtet, die geheimen Daten nicht unverschlüsselt über das Netz zu versenden, sondern Verschlüsselungstechnik einzusetzen."[1618]

Aus den Verschwiegenheitsverpflichtungen von Berufsgeheimnisträgern folgt daher eine Verschlüsselungspflicht bei der Übermittlung von Daten in unsicheren Umgebungen, insbesondere via Internet.

b. Verschlüsselungspflicht zur Gewährleistung der Datensicherheit?

Weiter ist zu untersuchen, ob Berufsgeheimnisträger aus ihrer Verschwiegenheitsverpflichtung über die Verschlüsselung bei Datenübermittlungen hinaus weitere Da-

stand eines Strafgesetzes verwirklicht, oder wenn sie bei sinngemäßer Umstellung des Sachverhalts auch nach deutschem Recht eine solche Tat wäre." Viele Entwicklungs- und Schwellenländer verfügen (noch) nicht über eine entsprechende Gesetzgebung von Straftaten im Internet.

1615 *Lindloff*, E-Mail-Kommunikation von Rechtsanwälten mit Mandanten und Gerichten, S. 104.

1616 Vergleiche dazu auch *Scherf*, in: *Scherf/Schmieszek/Viefhues*, Elektronischer Rechtsverkehr, C.III, Rn. 12.

1617 Vgl. die ausführlichen Überlegungen zum Sicherheitsniveau verwendeter Verschlüsselungsverfahren *Wagner/Lerch,* NJW-CoR 1996, 380, 384 f.

1618 *Speichert*, Praxis des IT-Rechts, S. 243.

tensicherheitsmaßnahmen zu treffen verpflichtet sind. Zwei Dinge sind dabei zu beachten:

- Zum einen ist neben dem Vertraulichkeitsschutz auch an einen vorgelagerten Integritätsschutz zum Zwecke des Vertraulichkeitsschutzes zu denken (wie vom BVerfG hinsichtlich des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entwickelt).
- Zum zweiten kann einem Berufsgeheimnisträger nur dann eine Verletzung seiner Verschwiegenheitsverpflichtung vorgeworfen werden, wenn er mindestens fahrlässig gehandelt hat (auf der strafrechtlichen Ebene wäre sogar – zumindest bedingter – Vorsatz erforderlich). Fahrlässig handelt nach § 276 II BGB, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt. Die erforderliche Sorgfalt bestimmt sich dabei „nach dem Urteil besonnener und gewissenhafter Angehöriger des in Betracht kommenden Verkehrskreises."[1619] An den Verkehrskreis der verschwiegenheitsverpflichteten Berufsgeheimnisträger kann man dabei – verglichen mit dem Durchschnittsbürger – durchaus erhöhte Anforderungen bezüglich der Gewährleistung von Vertraulichkeit stellen.[1620]

Grundsätzlich ist der Maßstab der technisch-organisatorischen Sicherheit nach der Anlage zu § 9 S. 1 BDSG anzuwenden, da Berufsgeheimnisträger als nichtöffentliche Stellen nach § 1 II Nr. 3 BDSG in den Anwendungsbereich des BDSG fallen, soweit sie personenbezogene Daten in Datenverarbeitungsanlagen verarbeiten oder nutzen.[1621] Die Kanzlei- oder Praxis-EDV muss also durch Maßnahmen der Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle den Schutz der personenbezogenen Daten gewährleisten. Daran zeigt sich, dass die Behauptung, Berufsgeheimnisträger seien zu aktiven Sicherheitsmaßnahmen wie dem Einbau von Sicherheitsschlössern oder Safes nicht verpflichtet (s.o.), schlicht falsch ist: Derartige Maßnahmen können durchaus zu einem IT-Sicherheitskonzept, wie es das BDSG verlangt, gehören.[1622]

> "Hierzu gehört für den virtuellen Bereich insbesondere auch die Herstellung von sicheren Kommunikationswegen. Die angesprochenen Berufsgruppen dürfen daher ihr Intranet nicht

1619 *Heinrichs*, in: *Palandt,* BGB, § 276, Rn. 16.

1620 So wurde etwa unter Journalisten ein Kodex mit einzuhaltenden Minimalstandards bei der Online-Recherche diskutiert. Bestandteil sollte auch eine Anonymisierungspflicht sein: „Techniken und Programme der Anonymisierung (wie etwa TOR, Jondos, Proxies, Remailer) sind daher ein Muss für recherchierende Journalisten."; zitiert nach heise online vom 07.06. 2009, Journalisten und Blogger gegen den Datentrash, verfügbar unter: http://www.heise.de/newsticker/Journalisten-und-Blogger-gegen-den-Datentrash--/meldung/140034 (08.06. 2009).

1621 Spindler, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, verfügbar unter: https://www.bsi.bund.de/cae/servlet/contentblob/486890/publicationFile/30666/Gutachten_pdf.pdf;jsessionid=A2EBB4098A4A5164D2E86814BBC18AEC (04.09.2009), S. 253.

1622 Vgl. etwa in den IT-Grundschutzkatalogen des BSI die Abschnitte zu Verwendung von Sicherheitstüren und –fenstern (M 1.10), Einbruchsschutz (M 1.19), Abgeschlossene Türen (M 1.123), Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz (M 1.134), Sichere Aufbewahrung der Datenträger vor und nach Versand (M 1.136), Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger (M 1.145), Einsatz von Diebstahl-Sicherungen (M 1.146); verfügbar unter http://www.bsi.de/gshb/deutsch/m/m01.htm (06.02. 2009).

ungeschützt ans Internet anhängen, sondern müssen die notwendigen Vorkehrungen zur Schaffung von IT-Sicherheit treffen. Maßnahmen, die in einem verhältnismäßigen Umfang geeignet sind, das Ausspähen geheimer Daten durch Hackerangriffe zu verhindern, wie etwa eine Firewall, sind erforderlich."[1623]

Berufsrechtliche Verschwiegenheitsverpflichtungen erfordern also in der Regel auch Maßnahmen der Datensicherheit, insbesondere auch durch Verschlüsselung.[1624]

2. Verschlüsselung zum Schutz von Betriebs- und Geschäftsgeheimnissen?

Anders ist dies bei Betriebs- und Geschäftsgeheimnissen. In der Regel sind keine personenbezogenen Daten betroffen. Daher ist zu prüfen, inwieweit sich auch zum Schutz von Betriebs- und Geschäftsgeheimnissen Verschlüsselungspflichten ergeben können.

a. Geheimnisschutz im eigenen Verantwortungsbereich

Zunächst geht es bei einem Großteil der IT-Sicherheitsfragen nicht um den Schutz fremder Interessen und Geheimnisse, sondern allein um den Schutz der unternehmens*eigenen* Betriebs- und Geschäftsgeheimnisse. Für die Wahrnehmung eigener Interessen von Wirtschaftssubjekten[1625] treffen den Staat geringere Schutzpflichtanforderungen. Zwar muss er die zu Grunde liegende eigentumsrechtliche Rechtsposition rechtlich anerkennen und entsprechend zivil-, straf- und öffentlich-rechtlich schützen.[1626] Die praktische Wahrnehmung und Umsetzung dieses rechtlichen Schutzes kann er aber durchaus den betroffenen Wirtschaftssubjekten selbst überlassen. Da es um den Schutz eigener Rechtsgüter im eigenen Interesse geht, wird man vom Staat keine darüber hinausgehenden Informationspflichten o.ä. verlangen können.[1627] Schließlich existieren umfangreiche Informationsangebote des BSI, etwa die IT-Grundschutz-Kataloge. Weitergehende staatliche Unterstützung bei der Umsetzung solcher Schutzmaßnahmen ist aus der grundrechtlichen Schutzpflichtenperspektive nicht erforderlich. Wirtschaftssubjekten ist es – im Gegensatz zu Privatpersonen – auch ohne Weiteres zumutbar, sich erforderliches weitergehendes Know-how einzukaufen. Da die erforderlichen technisch-organisatorischen Maßnahmen

1623 *Speichert*, Praxis des IT-Rechts, S. 243.

1624 So wird in der Diskussion um die elektronische Gesundheitskarte beispielsweise durch die Betreibergesellschaft der Gesundheitskarte ganz selbstverständlich davon ausgegangen, dass „der Arzt immer noch selbst für die Sicherheit seiner Daten zuständig sei“ (Jakobs, TP: Der offene Arzt-PC: "Hereinspaziert!", verfügbar unter: http://www.heise.de/tp/r4/artikel/30/30350/1.html (19.05.2009)).

1625 Anders kann dies etwa beim weniger gut informierten und vor allem weniger mächtigen Verbraucher zu bewerten sein.

1626 Einen Überblick gibt *Kloepfer,* Informationsrecht, § 9, Rn. 11 ff.

1627 Ähnlich auch *Kloepfer,* Informationsrecht, § 9, Rn. 19.

zum Schutz von personenbezogenen Daten und von Geheimnissen grundsätzlich übereinstimmen, kann zusätzlich auch auf Beratungsangebote von Datenschutzbeauftragten oder ein Datenschutzaudit zurückgegriffen werden. Rechtsgüter Dritter, denen der Staat eventuell weitergehenden Schutz schulden könnte, sind jedenfalls in der Regel nicht betroffen; ein weitergehendes staatliches Schutzkonzept ist nicht erforderlich.

b. Geheimnisschutz im fremden Verantwortungsbereich

Gleichwohl muss der Staat natürlich Sorge dafür tragen, dass Betriebs- und Geschäftsgeheimnisse *innerhalb des staatlichen Kenntnisbereichs* ausreichend geschützt werden. Dementsprechend ist auch das unbefugte Offenbaren von Betriebs- und Geschäftsgeheimnissen durch Amtsträger nach § 203 II S. 1, Nr. 1 StGB strafbar.[1628] Ein unbefugtes Offenbaren kann auch im Unterlassen von Sicherheitsvorkehrungen liegen.[1629] Die erforderliche Garantenstellung liegt bei Amtsträgern jedenfalls vor. Voraussetzung ist aber in jedem Fall vorsätzliches Unterlassen. Es ist jedoch äußerst fraglich, inwieweit die gesamte Organisationsstruktur einer Behörde einzelnen Amtsträgern zugerechnet werden könnte.[1630] Ein fehlendes (IT-)Sicherheitskonzept wird also kaum eine Strafbarkeit begründen können.

Jenseits strafrechtlicher Sanktionsnormen ist etwa der Zugang zu amtlichen Informationen, die Betriebs- und Geschäftsgeheimnisse enthalten, nur mit Einwilligung des Betroffenen zu erteilen (§ 6 IFG).[1631] Im verwaltungsgerichtlichen (§ 99 I VwGO) und im finanzgerichtlichen (§ 86 I, II FGO) Verfahren existiert ein in-camera-Verfahren, um die Geheimhaltung zu gewährleisten.[1632] Auch bereits im behördlichen Verfahren wird Akteneinsicht nur gewährt, wenn keine entgegenstehenden berechtigten Geheimhaltungsinteressen bestehen (§ 29 II VwVfG). Die Verfahrensbeteiligten haben einen Geheimhaltungsanspruch (§ 30 VwVfG). Spezielle Geheimhaltungsregelungen für Betriebs- und Geschäftsgeheimnisse existieren darüber hinaus in Bereichen besonderen Geheimhaltungsbedürftigkeit, etwa in § 17a Gentechnikgesetz.

1628 Für Betriebs- und Geschäftsgeheimnisse im Zusammenhang mit Steuersachen gilt Entsprechendes, § 355 I Nr. 2 StGB.

1629 So *Cierniak*, in: *Joecks/Miebach,* MüKo StGB, 203, Rn. 52: „Strafbares Unterlassen kann gegeben sein, wenn der Schweigepflichtige das Aufrufen bestimmter Dateien nicht verhindert."

1630 Anders könnte dies für einen zivilrechtlichen Amtshaftungsanspruch nach § 839 BGB i.V.m. Art. 34 GG unter dem Gesichtspunkt des Organisationsverschuldens zu sehen sein. Vgl. zur Haftung für Organisationsmängel – allerdings hinsichtlich der (personellen) Ausstattung von Gerichten – BGH, Urteil vom 11.01.2007, Az: III ZR 302/05, NJW 2007, 830, 832 f.

1631 Besondere Schutzvorschriften für Betriebs- und Geschäftsgeheimnissen enthalten auch § 9 I Nr. 3 UIG und § 5 III S. 1, Nr. 3 Gesetz zur Ausführung des Protokolls über Schadstofffreisetzungs- und -verbringungsregister vom 21. Mai 2003 sowie zur Durchführung der Verordnung (EG) Nr. 166/2006 vom 6. Juni 2007 (BGBl. I S. 1002).

1632 Zum Ablauf des in-camera-Verfahren siehe § 99 II VwGO.

Bei diesen Vertraulichkeitsregelungen geht es allerdings weniger um allgemeine Grundsätze der (Sicherheit der) Aktenaufbewahrung oder Datenarchivierung, sondern um den Umgang mit Akteneinsichtsrechten sowie Übermittlungspflichten. Spezielle Anforderung hinsichtlich der zu gewährleistenden Sicherheit behördlicher Informationen (seien es Akten in Papierform oder Daten) existieren nicht. Es gibt keinerlei Regelungen, die technisch-organisatorische IT-Sicherheitsmaßnahmen (etwa in Anlehnung an den Katalog der Anlage zu § 9 S. 1 BDSG) zur Gewährleistung der Vertraulichkeit fremder Geheimnisse festlegen. Elektronische Kommunikation mit Behörden wird zwar ermöglicht, spezielle diesbezügliche Vertraulichkeitsanforderungen – geschweige denn Verschlüsselungspflichten – aber nicht gestellt.[1633]

Eine solche Verschlüsselungspflicht ergibt sich aber aus dem Geheimhaltungsanspruch nach § 30 VwVfG.[1634] Wie schon hinsichtlich des Schutzes des Fernmeldegeheimnisses (Art. 10 I GG) sowie des Schutzes von Berufsgeheimnissen (Art. 12 I GG) dargelegt, verlangen solche Vertraulichkeits- oder Geheimhaltungsregelungen[1635] in verfassungskonformer Auslegung den Einsatz von Verschlüsselungsverfahren, um

- Vertraulichkeit bzw. Geheimhaltung in unsicheren Umgebungen, etwa bei Datenübermittlung über Internet, sicherzustellen sowie
- die Integrität behördlicher informationstechnischer Systeme zu gewährleisten, um einer Infiltration (mit anschließender unbefugter Kenntnisnahme von Daten) vorzubeugen.

Auch hier kann hinsichtlich der technisch-organisatorischen Anforderungen auf die Anlage zu § 9 S. 1 BDSG zurückgegriffen werden.

1633 Siehe § 3a VwVfG: „ [Elektronische Kommunikation] (1) Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet. (2) Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht ermöglicht, ist nicht zulässig. (3) Ist ein der Behörde übermitteltes elektronisches Dokument für sie zur Bearbeitung nicht geeignet, teilt sie dies dem Absender unter Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mit. Macht ein Empfänger geltend, er könne das von der Behörde übermittelte elektronische Dokument nicht bearbeiten, hat sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück zu übermitteln.“

1634 § 30 VwVfG normiert einen allgemeinen Rechtsgedanken und ist daher auch jenseits des Anwendungsbereichs des VwVfG auf öffentlich-rechtliche Verwaltungstätigkeit anwendbar; *Herrmann*, in: *Bader/Ronellenfitsch,* BeckOK VwVfG, § 30, Rn. 7.

1635 Geheimhaltung und Vertraulichkeit können insoweit gleichgesetzt werden: Beides bedeutet im Kern „Schutz vor unbefugter Kenntnisnahme“.

c. Geheimnisschutz gegenüber Dritten innerhalb des eigenen Verantwortungsbereichs

Die Vertraulichkeit von Betriebs- und Geschäftsgeheimnissen kann schließlich auch aus der unternehmenseigenen Sphäre bedroht werden – durch eigene oder ehemalige Mitarbeiter und Geschäftspartner. Auch diese sind Dritte, vor deren Eingriffen in eigentumsrechtliche Rechtspositionen der Staat Schutz gewährleisten muss. So ist eine Vertraulichkeitsverpflichtung des Arbeitsnehmers als Nebenpflicht aus dem Arbeitsverhältnis, § 241 II BGB, anerkannt.[1636] Vor- und nachvertragliche Vertraulichkeitsverpflichtungen können sich ebenfalls aus arbeitsvertraglichen Nebenpflichten ergeben oder allgemeiner aus dem Grundsatz von Treu und Glauben, § 242 BGB.[1637] Mit Geschäftspartnern sollten dagegen gesonderte vertragliche Vertraulichkeitsabreden getroffen werden, auch wenn sich derartige Vertraulichkeitsverpflichtungen ebenfalls aus Treu und Glauben ergeben können.

Damit liegt auch hier der Schutz der Vertraulichkeit in Händen des Geheimnisinhabers: Es liegt am Inhaber eines Betriebs- und Geschäftsgeheimnisses selbst, ob er ein entsprechendes IT-Sicherheitskonzept implementiert, dass einen Vertraulichkeitsbruch durch Unbefugte von außen verhindert sowie mögliche Innentäterattacken erschwert. Auch eine entsprechende Vertragsgestaltung liegt allein im Interesse und in Händen des Geheimnisinhabers. Der Staat hat die entsprechenden Normen und Voraussetzungen jedenfalls geschaffen. Zudem existieren Straftatbestände, die das Offenbaren von Betriebs- und Geschäftsgeheimnissen pönalisieren.

d. Zusammenfassung

Insgesamt ergeben sich *für Private* (seien es natürliche oder juristische Personen) *keine* speziellen Verschlüsselungsgebote zum Schutz von Betriebs- und Geschäftsgeheimnissen. Die Geheimhaltung betrifft nur eigene Geheimnisse, eigene Interessen oder eigene (vertragliche) Obliegenheiten. Schutzbedürftige Interessen außenstehender Dritter sind nicht betroffen. Da sich die zu schützenden Geheimnisse in der eigenen Sphäre des Geheimnisinhabers befinden oder von diesem bewusst an Geschäftspartner oder andere Dritte weitergegeben werden, so obliegt es ihm selbst, für einen entsprechenden Schutz zu sorgen. Die rechtlichen und tatsächlichen Voraussetzungen hierfür hat der Gesetzgeber in ausreichendem Maße geschaffen.

Befinden sich Betriebs- und Geschäftsgeheimnisse *hingegen innerhalb der staatlichen Sphäre* – und damit außerhalb der Kontrolle und unter Umständen ohne entsprechenden Willen des Geheimnishabers – *muss der Staat ihre Vertraulichkeit sicherstellen*. Diesen Interessen tragen etwa besondere Vorschriften zu Aktenein-

1636 *Weidenkaff*, in: *Palandt,* BGB, § 611, Rn. 39, 41.

1637 *Heinrichs*, in: *Palandt,* BGB, § 242, Rn. 23. Das Verhältnis von § 242 BGB und § 241 II BGB scheint insoweit noch nicht abschließend geklärt zu sein, in der Sache geht es aber um denselben Rechtsgedanken.

sichtsrechten oder Übermittlungspflichten Rechnung. Aus dem allgemeinen Rechtsgrundsatz der Geheimhaltungspflicht für Betriebs- und Geschäftsgeheimnisse ergibt sich in verfassungskonformer Auslegung eine Verschlüsselungspflicht zur Gewährleistung der Geheimhaltung in unsicheren Umgebungen sowie zur Sicherstellung der Integrität informationstechnischer Systeme.

III. Bedeutung der Perspektive wirtschaftlicher Grundrechte für Verschlüsselungspflichten und -rechte

Die Frage, ob der Staat seinen Schutzpflichten für Betriebs- und Geschäftsgeheimnisse sowie Berufsgeheimnisse ausreichend Genüge getan hat mit den soeben vorgestellten Schutzkonzepten, bringt in der Sache wenig Neues:

- Der Schutz von Berufsgeheimnissen nähert sich hier dem Schutz des allgemeinen Persönlichkeitsrechts an. Bei Art. 12 I GG sind parallele Standards wie im Rahmen von Art. 2 I GG i.V.m. Art. 1 I GG zu gewährleisten, die tatsächlichen Anforderungen orientieren sich jeweils an den Maßnahmekatalogen der technisch-organisatorischen Sicherheit und es sind parallele Abwägungsentscheidungen zu treffen. Wie im Rahmen des Schutzes des allgemeinen Persönlichkeitsrechts sind entsprechende Maßnahmen zur Gewährleistung der Vertraulichkeit und Integrität von Daten und informationstechnischen Systemen nicht nur von staatlichen Stellen, sondern vor allem auch von Privaten zu gewährleisten. Dies sind hier die Berufsgeheimnisträger bzw. in deren Sphäre tätige Personen. Deren einfachgesetzliche Vertraulichkeitsverpflichtung verdichtet sich in verfassungskonformer Auslegung zu einer Verschlüsselungspflicht sowohl bei Datenübermittlungen in unsicheren Umgebungen wie zur Sicherstellung der Systemintegrität. Dass die verfassungskonforme Auslegung der standesrechtlichen Verschwiegenheitsverpflichtungen kein ausreichendes staatliches Schutzkonzept darstellt, verdeutlicht die in der Literatur geführte Debatte darüber, ob Berufsgeheimnisträger Verschlüsselungspflichten treffen oder nicht, nachdrücklich. Wurde schon das vornehmlich über die Datenschutzgesetze konkretisierte Schutzkonzept hinsichtlich des allgemeinen Persönlichkeitsrechts als nicht hinreichend effektiv eingestuft, gilt dies für den Schutz von Berufsgeheimnissen umso mehr: Hierfür existieren noch nicht einmal eigene Normen zum Geheimnisschutz und den dazu notwendigen technisch-organisatorischen Maßnahmen, sondern die bereits an sich vagen und daher kritikwürdigen Datenschutznormen werden zur Ausfüllung konkretisierungsbedürftiger Rechtsbegriffe aus zivil-, straf- und standesrechtlichen Normen herangezogen.
- Zum Schutz von Betriebs- und Geschäftsgeheimnissen (Art. 14 I S. 1 GG) durch Private besteht ein ausreichendes staatliches Schutzkonzept. Es ist nicht zu beanstanden, dass der Gesetzgeber sich darauf beschränkt, den Schutz von Betriebs- und Geschäftsgeheimnissen rechtlich anzuerkennen und – etwa durch strafrechtliche Sanktionen – zu gewährleisten, die praktische Umsetzung durch

Implementierung von (IT-)Sicherheitsvorkehrungen aber den Betroffenen selbst zu überlassen.

Soweit sich Betriebs- und Geschäftsgeheimnisse in staatlicher Hand befinden, muss der Staat deren Schutz allerdings gewährleisten. Auch wenn in der Regel keine personenbezogenen Daten betroffen sind, kann dennoch auch hier eine parallele Betrachtung wie beim allgemeinen Persönlichkeitsrecht vorgenommen werden. Die zu schützenden Daten sind ebenfalls sensibel, nur nicht im Hinblick auf ihren Personenbezug, sondern wegen ihrer wirtschaftlichen Bedeutung für den Geheimnisträger. Das vorhandene staatliche Schutzkonzept ist insoweit nicht ausreichend. Es existiert zwar ein allgemeiner Rechtsgedanke, der sich vor allem in § 30 VwVfG niedergeschlagen hat, wonach ein Geheimhaltungsanspruch besteht. Es gibt aber keine konkreteren Vorschriften, welche Anforderungen sich aus diesem allgemeinen Rechtsgrundsatz für staatliche Stellen ergeben: So existieren weder allgemeine Normen zum Geheimnisschutz, wie es sie etwa mit den Datenschutzgesetzen für personenbezogene Daten gibt. Auch ein vergleichbarer Katalog erforderlicher technisch-organisatorischer Maßnahmen existiert nicht. Sonstige gesetzliche Regelungen, die sich mit Geheimhaltung beschäftigen, regeln vor allem den Umgang mit Akteneinsichtsrechten oder Übermittlungspflichten. Die Sicherheit von Akten- oder Datenverwaltung und -aufbewahrung ist dagegen nicht geregelt. Die verfassungskonforme Anwendung eines allgemeinen Rechtsgedankens kann als staatliches Schutzkonzept nicht ausreichen. Diese Einschätzung wird durch praktische Beispiele fehlenden behördlichen Problembewusstseins bestätigt, etwa die bereits dargelegte mangelnde Implementierung von Verschlüsselungsvorgaben für den elektronischen Rechtsverkehr.

Die Perspektive der wirtschaftlichen Grundrechte besitzt trotz zahlreicher Parallelen zum Schutz durch das Fernmeldegeheimnis (Art. 10 I GG) und das allgemeine Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) und gewisser Redundanzen auch eigenständige Bedeutung:

- Zum einen wird der *Kreis der Grundrechts- und damit Schutzberechtigten erweitert*. Im Gegensatz zum allgemeinen Persönlichkeitsrecht (zumindest in den hier relevanten Ausprägungen) schützen Eigentums- und Berufsfreiheit auch juristische Personen.
- Zum anderen können *zusätzliche Personen* Schutz beanspruchen: Mit den Berufsgeheimnissen werden sowohl die eigene Grundrechtsposition der Berufsgeheimnisträger (Art. 12 I GG) als auch die Grundrechtsposition ihrer Mandanten, Klienten, Patienten, Informanten etc. (allgemeines Persönlichkeitsrecht, Art. 2 I GG i.V.m. Art. 1 I GG) geschützt. Der sich auf den Schutz seines Berufsgeheimnisses berufende Geheimnisträger nimmt damit einerseits eigene Rechte wahr, andererseits ist dies gleichzeitig ein vorgelagerter Schutz des allgemeinen Persönlichkeitsrechts seiner Klienten.
- Eine *Ausweitung des Grundrechtsschutzes* ergibt sich auch *hinsichtlich des Schutzgegenstandes*: Schutz wird nicht ausschließlich für personenbezogene, sondern auch für nicht personenbezogene, aber gleichwohl geheimhaltungsbedürftige Daten gewährt.

C. Verschlüsselung und „gute Verwaltung“

Auch wenn es zwar kein allgemeines „Grundrecht auf Sicherheit“[1638] gibt, könnte sich doch zumindest ein allgemeines „Grundrecht auf IT-Sicherheit“ als Ausprägung eines aus dem Rechtsstaatsprinzip (Art. 20 III GG) abzuleitenden Rechts auf gute Verwaltung ergeben. Ein derartiges Recht auf gute Verwaltung würde auch Grundsätze zum Umgang mit Daten umfassen, wie etwa Art. 9 Recommendation CM/Rec (2007)7 of the Committee of Ministers to member states on good administration vom 20.06.2007[1639] und Art. 21 des Europäischen Kodex für gute Verwaltungspraxis[1640] zeigen.

I. „Recht auf gute Verwaltung“ als Teil des Rechtsstaatsprinzips (Art. 20 III GG)?

So wie Art. 41 der europäischen Grundrechtecharta ausdrücklich ein Recht des Einzelnen auf eine gute Verwaltung nennt, könnte es auch auf nationaler Ebene ein entsprechendes Grundrecht auf gute Verwaltung geben. Ausdrücklich ist ein Grundrecht auf gute Verwaltung nicht im Grundgesetz vorgesehen. Dies ist nicht verwunderlich, da das Konzept der „guten Verwaltung“ oder „guten Verwaltungstätigkeit“ (`*good administration*´) auf dem breiteren Konzept der „guten Regierungsführung“

1638 Die Bezeichnung erlangte vor allem durch die Publikation von *Isensee*, Das Grundrecht auf Sicherheit, Bekanntheit. Es geht dabei aber nicht um die Deduktion eines neuen Grundrechts (vgl. umfassend zur Kritik an einem solchen Grundrecht *Kutscha*, Innere Sicherheit und Freiheitsrechte, in: *Roggan/Kutscha,* Handbuch zum Recht der Inneren Sicherheit, S. 28, 31 ff.), sondern vielmehr um eine neue, allen Grundrechten innewohnende Dimension, die staatliche Schutzpflicht: „Der Gewinn, den man aus der Argumentationsfigur des "Grundrechts auf Sicherheit" ziehen kann, liegt darin, dass deutlich wird, dass die effektive Gewährleistung von Grundrechtsgütern ein aktives Tun, eine Schutzbemühung des Staates voraussetzt, die in der Wirklichkeit wirksam ist. Der Erkenntnisgewinn liegt auch in der Akzentuierung, dass die Tätigkeit der Polizei und der staatlichen Behörden im Bereich des Umweltschutzes dem Einzelnen geschuldet ist, soweit seine Grundrechte betroffen sind und eine Schutzpflicht besteht.“; *Stoll*, Sicherheit als Aufgabe von Staat und Gesellschaft, S. 5.

1639 “Article 9 – Principle of respect for privacy: 1. Public authorities shall have respect for privacy, particularly when processing personal data. 2. When public authorities are authorised to process personal data or files, particularly by electronic means, they shall take all necessary measures to guarantee privacy. 3. The rules relating to personal data protection, notably as regards the right to have access to personal data and secure the rectification or removal of any data that is inaccurate or shall not have been recorded, shall apply to personal data processed by public authorities.”

1640 Artikel 21 [Datenschutz]: „1. Der Beamte, der mit personenbezogenen Daten umgeht, die einen Bürger betreffen, beachtet die Privatsphäre und die Unversehrtheit der Person gemäß den Bestimmungen der Verordnung (EG) Nr. 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und den freien Datenverkehr. 2. Der Beamte sieht insbesondere davon ab, personenbezogene Daten für unrechtmäßige Zwecke zu verarbeiten bzw. solche Daten an unbefugte Personen weiterzuleiten.“

(`*good governance´*) basiert,[1641] welches erst in den 80er Jahren – im Zusammenhang mit der internationalen Entwicklungspolitik – aufkam.[1642] Daher könnte die Notwendigkeit einer dynamischen Verfassungsinterpretation gegeben sein. Als verfassungsrechtlicher Anknüpfungspunkt bietet sich dabei das Rechtsstaatsprinzip (Art. 20 III GG) an, da zentrale Grundsätze eines „Rechts auf gute Verwaltung" unter das Rechtsstaatsprinzip fallen:[1643] etwa der Grundsatz der Gesetzesmäßigkeit der Verwaltung,[1644] der Grundsatz der Verhältnismäßigkeit,[1645]das Recht auf Anhörung,[1646] das Recht auf Entscheidungsbegründung[1647] und der Grundsatz der Unparteilichkeit.[1648]

Etliche Komponenten eines „Rechts auf gute Verwaltung" sind also bereits de lege lata verfassungsrechtlich verbürgt, zum Teil auch in anderen Normen des Grundgesetzes wie etwa der Grundsatz der Nichtdiskriminierung (Art. 5 des Europäischen Kodex für gute Verwaltungspraxis; Art. 3 GG). Hinsichtlich der genannten Grundsätze für staatliche Verwaltungstätigkeit und Rechte des Betroffenen ist die Herleitung und Anerkennung eines eigenständigen „Rechts auf gute Verwaltung" nicht erforderlich. Andere im Europäischen Kodex für gutes Verwaltungshandeln genannte Grundsätze und Rechte dürften dagegen einer verfassungsrechtlichen Fundamentierung – und zum Teil einer Verrechtlichung überhaupt – weniger zugänglich sein; etwa wo der Kodex folgerichtiges Handeln (Art. 10 des Kodex),[1649] Höflichkeit (Art.

1641 So ausdrücklich auch Recommendation CM/Rec(2007)7 of the Committee of Ministers to member states on good administration vom 20.06.2007, 20. Erwägungsgrund: "Considering that good administration is an aspect of good governance […]".

1642 Siehe Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung, http://www.bmz.de/de/them en/goodgovernance/guteregierung/hintergrund/index.html (23.02.2009).

1643 *Galetta,* EuR 2007, 57, 58.

1644 Im deutschen GG als Teil des Grundsatzes vom Vorrang des Gesetzes (Art. 20 III 2. Hs. GG), *Schulze-Fielitz*, in: *Dreier,* GG, Art. 20 (Rechtsstaat), Rn. 92; im europäischen Recht in Art. 4 des Europäischen Kodex für gute Verwaltungspraxis, der insoweit zur Konkretisierung von Art. 41 GRC herangezogen werden kann, vgl. *Magiera*, in: *Meyer,* GRC, Art. 41, Rn. 16.

1645 Vgl. für das deutsche Verfassungsrecht *Schulze-Fielitz*, in: *Dreier,* GG, Art. 20 (Rechtsstaat), Rn. 179 ff. sowie auf europäischer Ebene Art. 6 des Europäischen Kodex für gute Verwaltungspraxis.

1646 Im Grundgesetz als Teil des Grundsatzes des fairen Verfahrens, auf europäischer Ebene gem. Art. 41 II lit. a GRC.

1647 So ausdrücklich Art. 41 II lit. c GRC; siehe *Schulze-Fielitz*, in: *Dreier,* GG, Art. 20 (Rechtsstaat), Rn. 210; vgl. zu weiteren Anforderungen an Organisation und Verfahren der Verwaltung aus dem Rechtsstaatsprinzip *Schulze-Fielitz*, in: *Dreier,* GG, Art. 20 (Rechtsstaat), Rn. 204 ff.

1648 Vgl. *Schulze-Fielitz*, in: *Dreier,* GG, Art. 20 (Rechtsstaat), Rn. 209 sowie Art. 8 des Europäischen Kodex für gutes Verwaltungshandeln.

1649 Hierunter können auch verfassungsrechtlich relevante Sachverhalte fallen; so ist z.B. in Ziffer 2 („Der Beamte beachtet die berechtigten und billigen Erwartungen, die die Öffentlichkeit, in Anbetracht des Handelns des Organs in der Vergangenheit, hegt.") allgemeiner der Vertrauensschutzgedanke angesprochen, der – ebenfalls im Rechtsstaatsprinzip verankert – verfassungsrechtliche Relevanz haben kann.

12 des Kodex),[1650] den Versand von Empfangsbestätigungen und Kontaktdaten des zuständigen Ansprechpartners (Art. 14 des Kodex) oder die verpflichtende Weiterleitung an die zuständige Dienststelle (Art. 15 des Kodex) fordert.

Dies spricht im Ergebnis gegen die Herleitung eines eigenständigen Grundrechts auf gute Verwaltung, sei es aus dem Rechtsstaatsprinzip, sei es aus anderen Verfassungsnormen. Die zentralen Komponenten eines Rechts auf gute Verwaltung sind ohnehin verfassungsrechtlich verbürgt.[1651] Die Neuerungen des Ansatzes der `*good administration*´ sind dagegen gerade von „der Abkehr von einer ausschließlich an dem formalen Kriterium der Rechtmäßigkeit ausgerichteten Verwaltung hin zu einer auch an materiell guten Ergebnissen orientierten Verwaltung“[1652] geprägt. Es geht also bereits vom Denkansatz her gar nicht um die Verrechtlichung zusätzlicher Anforderungen an Verwaltungshandeln, sondern vielmehr um die Beseitigung bestehender Verwaltungsdefizite durch neue kooperative Mechanismen der Zusammenarbeit zwischen dem Einzelnen und dem Staat – weg vom kontradiktorisch geprägten gerichtlichen Rechtsschutz, hin zu weichen Rechtsdurchsetzungsmechanismen.

II. Schutzpflichtdimension des Rechtsstaatsprinzips?

Weiter wäre zu fragen, ob sich aus Verfassungsprinzipien[1653] wie dem Rechtsstaatsprinzip – im Unterschied zu verfassungsrechtlichen Grundrechten – überhaupt positive Schutzverpflichtungen für staatliche Stellen hinsichtlich Rechtsgutsverletzungen durch private Dritte entnehmen lassen. Dagegen spricht zum einen der objektive Prinzipiencharakter des Rechtsstaatsprinzips im Gegensatz zu den subjektiv geprägten Grundrechten. Das Rechtsstaatsprinzip umfasst Grundsätze, Regeln und Prinzipien, die „staatliche Machtausübung rechtlich binden, organisieren und begrenzen.“[1654] Der Regelungsgehalt betrifft also zum einen staatsorganisationsrechtliche Fragen, die keinen konkreten Bezug zum Einzelnen aufweisen (etwa der Grundsatz der Gewaltenteilung[1655]), und zum anderen klassisch abwehrrechtliche Konstellationen im Verhältnis des Einzelnen zum Staat (Vertrauensschutz, Rechtsgebundenheit staatlicher Stellen und Rechtmäßigkeit staatlichen Handelns, Rechtsschutzgarantie, rechtliches Gehör, gesetzlicher Richter etc.[1656]). Sicherlich ist dem Rechtsstaatsprinzip der Gedanke, dass der Staat den Grundrechtsberechtigten auch Schutz vor Rechtsgutsverletzungen durch private Dritte schuldet, durchaus inhärent. *Hermes*[1657] betont jedoch zu Recht, dass das Rechtsstaatsprinzip zwar etwas über Organisation

1650 Insbesondere das Verlangen nach Höflichkeit dürfte einer über die bereits bestehende Strafbarkeit von Beleidigungen hinaus gehenden Verrechtlichung nur schwer zugänglich sein.
1651 So auch *Bourquain,* DVBl. 2008, 1224, 1227.
1652 *Bourquain,* DVBl. 2008, 1224, 1225.
1653 Zur Terminologie siehe *Dreier*, in: *Dreier,* GG, Art. 20 (Einführung), Rn. 8 ff.
1654 *Schulze-Fielitz*, in: *Dreier,* GG, Art. 20 (Rechtsstaat), Rn. 38.
1655 Dazu *Schulze-Fielitz*, in: *Dreier,* GG, Art. 20 (Rechtsstaat), Rn. 67 ff.
1656 Aufzählung in Anlehnung an *Schulze-Fielitz*, in: *Dreier,* GG, Art. 20 (Rechtsstaat), Rn. 39.
1657 *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 129 ff, insbes. 133 f.

und Verfahren von Rechtsschutzmöglichkeiten aussagen mag, es regelt aber nur das „Wie" staatlichen Schutzes, und nicht das „Ob".[1658] Ob eine Person staatlichen Schutz gegenüber einer anderen Person beanspruchen kann, entscheidet aber nicht das Rechtsstaatsprinzip, sondern die zu Grunde liegende materielle (Grund-)Rechtsposition:

> „Es wird deutlich, daß dem Rechtsstaatsprinzip allein keine konkreten inhaltlichen Aussagen für die hier interessierende Problematik zu entnehmen sind. Zur Klärung dessen, was als Unrecht vom Staat zu verhindern ist, bleibt nur der Rückgriff auf grundrechtlich geschützte Rechtsgüter, die somit als normative Grundlage einer Schutzpflicht wieder in den Mittelpunkt rücken."[1659]

III. Keine Verschlüsselungspflicht als Teil eines „Rechts auf gute Verwaltung"

Folglich ergeben sich keine gesonderten Verschlüsselungs- oder sonstige Schutzpflichten aus einem aus dem Rechtsstaatsprinzip abzuleitenden „Recht auf gute Verwaltung". Erstens kann bereits kein allgemeines „Recht auf gute Verwaltung" aus dem Rechtsstaatsprinzip deduziert werden. Zweitens wären hier (beim Einsatz von Verschlüsselung gegen Angriffe privater Dritter) staatliche Schutzpflichten angesprochen; das Rechtsstaatsprinzip weist als Verfassungsprinzip aber keine eigenständige Schutzpflichtdimension auf. Zuletzt würden sich aus einem eigenständigen Grundrecht auf gute Verwaltung im Hinblick auf Verschlüsselungspflichten staatlicher Stellen keine zusätzlichen Anforderungen ergeben: Staatliche Stellen sind im Hinblick auf ihre umfassende Bindung an Recht und Gesetz (Art. 20 III GG) ohnehin zur Einhaltung datenschutzrechtlicher Normen gezwungen. Grundrechte, an die die Verwaltung ebenfalls gebunden ist (Art. 1 III GG), verstärken diesen Schutz, insbesondere für personenbezogene Daten (Recht auf informationelle Selbstbestimmung, Art. 2 I GG i.V.m. Art. 1 I GG), Kommunikationsdaten (Fernmeldegeheimnis, Art. 10 I GG), privatsphärenbezogene Daten (Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Art. 2 I GG i.V.m. Art. 1 I GG) sowie Betriebs- und Geschäftsgeheimnisse (Art. 14 I S. 1 GG).

Hinsichtlich all dieser Daten trifft den Staat

- eine allgemeine Pflicht zur Verschlüsselung bei Datenübermittlungen in unsicheren Umgebungen sowie
- eine Pflicht zur Gewährleistung der Datensicherheit.

Es sind kaum Konstellationen denkbar, in denen staatliche Stellen danach keinen Verschlüsselungspflichten unterliegen *und* gleichwohl Einzelne ein rechtlich beacht-

1658 Vgl. BSI: E-Government-Handbuch, „Rechtliche Rahmenbedingungen für E-Government", verfügbar unter: http://www.bsi.de/fachthem/egov/download/2_Recht.pdf (26.02.2008), S. 50: „Es bestehen keine speziellen rechtlichen Vorschriften über die notwendige Verfügbarkeit von technischen Systemen der Behörden. Auch aus allgemeinen Grundsätzen wie dem Rechtsstaatsprinzip lassen sich allenfalls Tendenzen, aber keine festen rechtlichen Vorgaben ableiten."

1659 *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 134.

liches Interesse an Verschlüsselung dieser Daten haben. Zu denken wäre allenfalls an den Schutz von Staatsgeheimnissen.[1660] Diese enthalten in der Regel keine der eben aufgezählten Datenkategorien, gleichwohl besteht durchaus ein Interesse jedes Einzelnen daran, dass Tatsachen, deren Bekanntwerden zu einer Bedrohung der Sicherheit des Staats führen kann, geheim gehalten werden. Dies ist aber kein Interesse des Einzelnen, dem auch ein subjektives Recht entspricht: Es gibt zwar eine Staatsaufgabe Sicherheit, dieser entspricht aber gerade kein Grundrecht auf Sicherheit.

Daher bleibt es bei dem durch die Schutzpflichtdimension der Einzelgrundrechte vermittelten Schutz. Ein darüber hinausgehendes „Recht auf gute Verwaltung" als Ausprägung des Rechtsstaatsprinzips (Art. 20 III GG) ist abzulehnen.

1660 Zum Begriff siehe § 93 I StGB [Begriff des Staatsgeheimnisses]: „(1) Staatsgeheimnisse sind Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht geheimgehalten werden müssen, um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden." Vgl. *Kloepfer,* Informationsrecht, § 7, Rn. 29.

Teil 7: Zusammenfassung und Ausblick

Verschlüsselungsverfahren sind in der digitalen Welt essentiell für den Schutz der Privatsphäre des Einzelnen wie auch für (nahezu) jede wirtschaftliche Betätigung. Jegliche Restriktionen der Nutzung von Verschlüsselungsverfahren (sowohl absolute als auch relative Verschlüsselungsverbote) verstoßen gegen multiple Grundrechte und geraten dabei in Konflikt mit

- Grundprinzipien unserer Rechtsordnung (Willkürverbot, Art. 3 I GG),
- der Basis unseres Wirtschaftssystems (Gewährleistung der wirtschaftlichen Betätigungsfreiheit durch Eigentums- und Berufsfreiheit, Art. 14 I GG und Art. 12 I GG)
- und den Kernwerten der Verfassung (Schutz der Menschenwürde in Art. 1 I GG sowie eines unantastbaren Kernbereichs privater Lebensgestaltung innerhalb von Spezialgrundrechten wie dem Fernmeldegeheimnis, Art. 10 I GG, dem Recht auf Unverletzlichkeit der Wohnung, Art. 13 I GG, und dem allgemeinen Persönlichkeitsrecht, Art. 2 I GG i.V.m. Art. 1 I GG).

Daher muss der Staat nicht nur jegliche Restriktion der Nutzung von Verschlüsselungsverfahren unterlassen, sondern ihren Einsatz darüber hinaus positiv fördern. Die derart gewährleistete Freiheit verkommt aber zur Farce, wenn sie nicht in Sicherheit gelebt werden kann (verfassungsrechtliche Schutzpflichten insbesondere für Leben und körperliche Unversehrtheit, Art. 2 II S. 1 GG). Unbeantwortet bleibt also weiterhin die Frage, wie der Staat adäquat mit den schwindenden Kenntnisnahmeoptionen seiner Sicherheitsbehörden in der digitalen Welt umgehen soll:

- Jegliche Art eines Verbots von Verschlüsselungsverfahren wäre verfassungswidrig (Teile 3 und 4).
- Die gesetzliche Implementierung einer Verpflichtung von Beschuldigten, verwendete Schlüssel oder Passwörter herauszugeben, wie sie etliche europäische Staaten vorsehen, verstieße gegen den nemo-tenetur-Grundsatz (Teil 5).
- Schließlich ist der Staat in einer verfassungsrechtlichen Perspektive verpflichtet, den Einsatz von Verschlüsselungsverfahren zu fördern. Prävention und Repression von Straftaten sowie die Sicherung des Rechtsfriedens stellen aber gleichermaßen einzulösende verfassungsrechtliche Verpflichtungen des Staates dar (Teil 6).

Wie diese Arbeit herausgearbeitet hat, scheiden Radikallösungen in der einen oder anderen Richtung – wie so oft im Spannungsfeld von Freiheit und Sicherheit – aus, da der Staat widerstreitende Anforderungen zu erfüllen aufgerufen ist, zwischen denen – immer wieder neu – eine angemessene Balance zu finden ist. Die Tendenzen können – angesichts der Unmöglichkeit befriedigender pauschaler Lösungen – insoweit nur verstärkt hin zu einer einzelfallbezogenen und differenzierten Betrachtung gehen. Derzeit zeichnen sich in Deutschland folgende Ansatzpunkte und Strategien ab:

Zum einen sind Strategien der Umgehung oder Überwindung im Einzelfall statt des generellen Verbots von Verschlüsselung in den Vordergrund gerückt: Während sich die Diskussion früher vorwiegend um die Angreifbarkeit bzw. die Schwächung der Verschlüsselungs*algorithmen* drehte, tendiert man heute eher zu dem Versuch, mittels `*Sniffer´*-Software oder `*keyloggern´* Schlüssel bzw. Passwörter auszuspähen, oder die Daten vor der Verschlüsselung bzw. nach der Entschlüsselung im Klartext zu erfassen.[1661] All diese Maßnahmen können unter dem Oberbegriff Online-Durchsuchung zusammengefasst werden, der definiert werden kann als ohne Wissen des Betroffenen erfolgenden Eingriff in von ihm genutzte informationstechnische Systeme und Datenerhebung aus diesen:

- Eine Rechtsgrundlage für die Online-Durchsuchung wurde zunächst in Nordrhein-Westfalen geschaffen. Die Regelung dieses § 5 II Nr. 11 VSG-NW[1662] wurde mittlerweile vom BVerfG für verfassungswidrig erklärt.[1663]
- Auf Bundesebene ist mit § 20k BKAG[1664] seit dem 01.01.2009 eine Rechtsgrundlage für die Online-Durchsuchung in Kraft.[1665]

1661 Bundesministerium des Innern, Fragenkatalog des Bundesministeriums der Justiz, verfügbar unter: http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (31.10.2007), S. 18 f.

1662 § 5 II Nr. 11 Verfassungsschutzgesetz Nordrhein-Westfalen i.d.F.v. 20.12.2006 lautete: „(2) Die Verfassungsschutzbehörde darf nach Maßgabe des § 7 zur Informationsbeschaffung als nachrichtendienstliche Mittel die folgenden Maßnahmen anwenden: (…) 11. heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel. Soweit solche Maßnahmen einen Eingriff in das Brief-, Post- und Fernmeldegeheimnis darstellen bzw. in Art und Schwere diesem gleichkommen, ist dieser nur unter den Voraussetzungen des Gesetzes zu Artikel 10 Grundgesetz zulässig; (…)“

1663 BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07 und 595/07.

1664 § 20k Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz - BKAG) vom 07. 07.1997 (BGBl. I S. 1650), zuletzt geändert durch Artikel 1 des Gesetzes vom 25.12.2008 (BGBl. I S. 3083): „[Verdeckter Eingriff in informationstechnische Systeme] (1) Das Bundeskriminalamt darf ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass eine Gefahr vorliegt für 1. Leib, Leben oder Freiheit einer Person oder 2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Eine Maßnahme nach Satz 1 ist auch zulässig, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass ohne Durchführung der Maßnahme in näherer Zukunft ein Schaden eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für eines der in Satz 1 genannten Rechtsgüter hinweisen. Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 4a erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre. […] (7) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme

- In Bayern wurde 2008 bei der Änderung des Polizeiaufgabengesetzes der „verdeckte Zugriff auf informationstechnische Systeme“ (Art. 34d PAG[1666]) zur Abwehr dringender Gefahren für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für andere gewichtige Rechtsgüter (Leib, Leben, Freiheit) eingeführt.[1667]
- In Hessen ist mit der am 08.12.2009 beschlossenen Novelle des HSOG eine Befugnis zu einer (präventiven) „Quellen-Telekommunikationsüberwachung“ eingeführt worden.[1668] Diese dient der Überwachung von Internettelefonie im Wege einer Infiltration der verwendeten informationstechnischen Systeme – insbesondere, wenn die Kommunikation verschlüsselt erfolgt. Eine solche Quellen-TKÜ erfordert ein ähnliches Vorgehen wie eine Online-Durchsuchung, da jeweils eine Infiltration des informationstechnischen Systems erfolgt.[1669]

unzulässig. Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erhobene Daten sind unter der Sachleitung des anordnenden Gerichts nach Absatz 5 unverzüglich vom Datenschutzbeauftragten des Bundeskriminalamtes und zwei weiteren Bediensteten des Bundeskriminalamtes, von denen einer die Befähigung zum Richteramt hat, auf kernbereichsrelevante Inhalte durchzusehen. Der Datenschutzbeauftragte ist bei Ausübung dieser Tätigkeit weisungsfrei und darf deswegen nicht benachteiligt werden (§ 4f Abs. 3 des Bundesdatenschutzgesetzes). Daten, die den Kernbereich privater Lebensgestaltung betreffen, dürfen nicht verwertet werden und sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.“

1665 Wobei auch diesbezüglich eine Verfassungsbeschwerde anhängig ist; der entsprechende Schriftsatz ist verfügbar unter: http://www.heise.de/tp/r4/artikel/29/29614/1.html (29.06. 2009).

1666 Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz – PAG) i.d.F. der Bekanntmachung vom 14.09.1990 (GVBl. 1990, 397), zuletzt geändert durch § 8 des Gesetzes vom 27. Juli 2009 (GVBl S. 400).

1667 Art. 34e PAG gestattete darüber hinaus als „notwendige Begleitmaßnahme“ das heimliche Betreten und Durchsuchen von Wohnungen. Diese Norm wurde aber zum 01.08.2009 wieder abgeschafft.

1668 Art. 1, Ziffer 8 des am 08.12.2009 beschlossenen Gesetzes zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze vom 30.06.2009, Drs. 18/861 fügt folgenden § 15b in das HSOG ein: „"§ 15b [Telekommunikationsüberwachung an informationstechnischen Systemen] (1) Wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist, kann die Überwachung und Aufzeichnung der Telekommunikation ohne Wissen der betroffenen Person in der Weise erfolgen, dass mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird, wenn 1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und 2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen. […]“

1669 Nach Angaben der Bundesregierung, vgl. BT-Drs 16/6885, S. 4; ausführlich zur Quellen-TKÜ siehe oben in Teil 3 unter A.III.1.f.aa)(3).

Allerdings bleiben die Problemfelder

- der (potentiellen) Betroffenheit von Daten aus dem unantastbaren Kernbereich privater Lebensgestaltung,
- des Zugriffs auf umfassende Datenbestände aus allen Lebensbereichen der Betroffenen sowie
- der daraus resultierenden Profilbildungsmöglichkeiten,

wie sie für Verschlüsselungsverbote existieren, auch für Online-Durchsuchungsmaßnahmen bestehen. Wie schon in seiner Entscheidung zur akustischen Wohnraumüberwachung[1670] hat das BVerfG daher auch für Online-Durchsuchungen hohe Hürden errichtet (Erfordernis einer konkreten Gefahr für ein überragend wichtiges Rechtsgut, Einhaltung verfahrensrechtlicher Anforderungen zur Gewährleistung des Kernbereichsschutzes). Angesichts dessen ist absehbar, dass die Online-Durchsuchung ebenso selten zum Einsatz kommen wird wie die akustische Wohnraumüberwachung.[1671] *Derart eingriffsintensive Maßnahmen werden wegen der Kernbereichsrelevanz immer äußerst restriktiv gehandhabt werden müssen*. Dies gilt auch für alle sonstigen denkbaren Angriffe auf IT-Systeme, etwa alle Formen von Seitenkanalangriffen. Solche Maßnahmen werden aus verfassungsrechtlichen Gründen immer auf Konstellationen, in denen bereits starke Verdachtsmomente für die Begehung schwerwiegender Straftaten existieren, reduziert bleiben. Für Strukturermittlungen aufgrund geringfügigerer Verdachtsmomente kommen derartige Instrumente nicht in Betracht. Gerade für diesen Bereich werden heimliche Kommunikationsüberwachungsmaßnahmen (etwa die TKÜ) gerne eingesetzt und aus kriminalistischer Sicht gefordert (s.o. in Teil 3 unter A.I.3.c.dd)(7).). Aus verfassungsrechtlichen Gründen kann es aber umfassende präventive oder lose verdachtsbasierte heimliche Überwachungsmaßnahmen nicht geben; das unterscheidet den freiheitlichen Rechtsstaat vom repressiven Polizei- oder Überwachungsstaat.

B. Strategien der Verlagerung des Verschlüsselungsvorgangs

Die zweite Strategie setzt daher mit einem Konzept der Freiwilligkeit auf die *Verlagerung* des Verschlüsselungsvorgangs weg von der von den Kommunikationsteilnehmern selbst vorgenommenen (sog. teilnehmerautonomen) Verschlüsselung hin zu Verschlüsselung durch Kommunikationsdiensteanbieter. Als Beispiel für Maßnahmen einer solchen Strategie kann etwa das geplante Bürgerportalgesetz[1672] die-

1670 BVerfG, Urteil vom 03.03.2004, Az.: 1 BvR 2378/98 und 1 BvR 1084/99.

1671 Laut heise online vom 26.11.2009, de Maizière: "Wenn mehr Fußball gespielt wird, braucht man mehr gelbe Karten", verfügbar unter: http://www.heise.de/newsticker/meldung/de-Maizi ere-Wenn-mehr-Fussball-gespielt-wird-braucht-man-mehr-gelbe-Karten-870161.html (08.12. 2009) wurden 2008 sieben Wohnraumüberwachungsmaßnahmen durchgeführt.

1672 Entwurf eines Gesetzes zur Regelung von Bürgerportalen und zur Änderung weiterer Vorschriften vom 08.04.2009, BT-Drs. 16/12598.

nen. Bürgerportale sollen Kommunikationsplattformen für rechtsverbindliche und vertrauliche Kommunikation sein:

„§ 1 Bürgerportalgesetz [Bürgerportal]

(1) Bürgerportale im Sinne dieses Gesetzes bilden eine elektronische Kommunikationsplattform im Internet, deren Dienste sicheren elektronischen Geschäftsverkehr für jedermann ermöglichen und das Internet als Mittel für rechtsverbindliches und vertrauliches Handeln ausbauen.

(2) Bürgerportale im Sinne dieses Gesetzes ermöglichen eine sichere Anmeldung, die Nutzung eines Postfach- und Versanddienstes für sichere elektronische Post und die Nutzung eines Verzeichnisdienstes sowie optional von Identitätsbestätigungs- und Speicherplatzdiensten. Ein Bürgerportal wird von einem nach diesem Gesetz akkreditierten Diensteanbieter betrieben."

Der Nutzer kann sich bei einem der akkreditierten Diensteanbieter ein E-Mail-Postfach einrichten; die E-Mails solcher Bürgerportale werden als De-Mail bezeichnet.[1673] Die E-Mail-Adresse soll dementsprechend ebenfalls auf `.de-mail.de´ enden.[1674] Die Bürgerportale bieten in der Hauptsache einen E-Mail-Postfach- und -Versanddienst an, optional ist die Nutzung von Verzeichnis-, Identitätsbestätigungs- und Speicherplatzdiensten[1675] möglich.

Hier interessiert vor allem, dass De-Mails stets vom Diensteanbieter für die Übermittlung verschlüsselt werden sollen, [1676] vgl. § 5 III Bürgerportalgesetz:

„§ 5 Bürgerportalgesetz [Postfach- und Versanddienst]

(3) Der Postfach- und Versanddienst hat die Vertraulichkeit, die Integrität und die Authentizität der Nachrichten zu gewährleisten."

Die De-Mails werden dabei aber lediglich beim Diensteanbieter des Absenders verschlüsselt und beim Diensteanbieter des Empfängers wieder entschlüsselt. Folglich wird nur für ein Teilstück des Kommunikationsweges die Vertraulichkeit gesichert, nämlich die Teilstrecke zwischen dem Bürgerportal des Absenders A und dem Bürgerportal des Empfängers E (Leitungsverschlüsselung[1677]):

$$\text{Absender A} \rightarrow \text{Bürgerportal A} \rightarrow \text{Bürgerportal E} \rightarrow \text{Empfänger E}$$

Der Zugang des Absenders A und des Empfängers B zu ihrem jeweiligen Bürgerportal wird dagegen nur optional durch eine sichere Anmeldung abgesichert:[1678]

1673 BT-Drs. 16/12598, S. 14.

1674 BT-Drs. 16/12598, S. 21.

1675 Vgl. § 8 Bürgerportalgesetz [Speicherplatz]: „Der akkreditierte Diensteanbieter kann dem Nutzer einen Speicherplatz zur sicheren Ablage von Dateien anbieten. Bietet er den Speicherplatz an, so hat er dafür Sorge zu tragen, dass die Ablage von Dateien sicher erfolgt. Der Nutzer kann für jede einzelne Datei eine für den Zugriff erforderliche sichere Anmeldung nach § 4 festlegen." Die Anforderungen an eine *sichere* Ablage werden gem. § 25 Nr. 8 Bürgerportalgesetz durch Rechtsverordnung geregelt; BT-Drs. 16/12598, S. 24. In der Sache dürfte aber eine Verschlüsselung der Daten erforderlich sein.

1676 BT-Drs. 16/12598, S. 21.

1677 S.o. in Teil 1 unter B.I.3.c.

1678 Darüber hinaus muss sich der Absender einer De-Mail nicht auf das Sicherheitsbewusstsein des Empfängers der De-Mail verlassen, sondern kann nach § 5 IV Bürgerportalgesetz festle-

„Die Sicherung der Vertraulichkeit, der Integrität und der Authentizität ist die Eigenschaft des Postfach- und Versanddienstes, die diesen von vergleichbaren Diensten unterscheidet. Aus diesem Grund ist sie ein Definitionsmerkmal dieses Bürgerportaldienstes. Die Sicherung erfolgt durch eine Verschlüsselung des Nachrichteninhaltes auf dem Transport zwischen den akkreditierten Diensteanbietern und durch die Sicherung des Zugangs zu den Bürgerportalen."[1679]

Selbst wenn dieser Modus der sicheren Anmeldung gewählt wird, bedeutet dies nur, dass die beiden Kommunikationswege vom Absender zu seinem Bürgerportal und vom Bürgerportal des Empfängers zum Empfänger *gesondert* abgesichert werden. *Die De-Mail liegt also zweimal unverschlüsselt im Klartext vor: einmal beim Bürgerportal des Absenders vor der Verschlüsselung zum Versand und einmal beim Bürgerportal des Empfängers nach der Entschlüsselung*. In diesen Momenten können die Diensteanbieter oder ihre Mitarbeiter Kenntnis vom Inhalt der De-Mail nehmen. Die Bürgerportale wären damit natürlich auch für Dritte (Geheimdienste, Kriminelle etc.) höchst interessante Stellen.[1680] Hier könnten – bei Schaffung einer entsprechenden Rechtsgrundlage – wie bei der Telekommunikationsüberwachung jeweils auch staatliche Sicherheitsbehörden auf die Daten zugreifen.

Zur Gewährleistung *echter* Vertraulichkeit von Kommunikationsinhalten ist aber stets eine Ende-zu-Ende-Verschlüsselung (vom Absender A bis zum Empfänger E) erforderlich – und nicht nur die vom Bürgerportal angebotene Transportsicherheit durch eine Leitungsverschlüsselung für einen Teil des Kommunikationsweges.[1681]

Zwar ist eine zusätzliche teilnehmerautonome Ende-zu-Ende-Verschlüsselung auch bei Nutzung von De-Mail möglich (und wird durch die Möglichkeit, Verschlüsselungsinformationen im Verzeichnisdienst gem. § 7 I Bürgerportalgesetz[1682] zu veröffentlichen, auch gefördert), sie ist aber gerade nicht standardmäßig vorgesehen.[1683] Dies wäre aber erforderlich, um tatsächlich vertrauliche Kommunikation zu gewährleisten. Dementsprechend fordert auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder:

„Die Sicherung der Vertraulichkeit, Integrität und Authentizität von Nachrichteninhalten soll lediglich durch eine Verschlüsselung auf dem Transport zwischen den Diensteanbietern und

gen, dass die Nachricht nur nach einer sicheren Anmeldung durch den Empfänger abgerufen werden kann.

1679 So der Gesetzesentwurf, BT-Drs. 16/12598, S. 22.

1680 Es können insoweit ähnliche Überlegungen wie für Infrastrukturen zur Aufbewahrung von hinterlegten Schlüsseln oder Nachschlüsselinformationen angestellt werden; s.o. in Teil 4 unter A.I.3.c.dd)(1).

1681 S.o. in Teil 1 unter B.I.3.c.

1682 § 7 Bürgerportalgesetz [Verzeichnisdienst]: „(1) Der akkreditierte Diensteanbieter hat auf ausdrückliches Verlangen des Nutzers die Bürgerportaladressen, nach § 3 hinterlegte Identitätsdaten sowie für die Verschlüsselung von Nachrichten an den Nutzer notwendige Informationen in einem Verzeichnisdienst zu veröffentlichen. Der akkreditierte Diensteanbieter darf die Eröffnung eines Bürgerportalkontos für den Nutzer nicht von dem Verlangen des Nutzers nach Satz 1 abhängig machen, wenn dem Nutzer ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne das Verlangen nicht oder nicht in zumutbarer Weise möglich ist."

1683 *Knopp/Wilke/Hornung/Laue,* MMR 2008, 723, 725.

durch die Sicherung des Zugangs zu den Bürgerportalen erfolgen. Es muss jedoch sichergestellt werden, dass Nachrichten auch bei den Portalbetreibern nicht durch Dritte gelesen oder verändert werden können. Deshalb muss die Kommunikation standardmäßig durch eine Ende-zu-Ende-Verschlüsselung zwischen Absendenden und Empfangenden nach dem Stand der Technik gesichert und nicht nur als Option angeboten werden."[1684]

Angesichts der Tatsache, dass derzeit der Großteil der Daten nach wie vor unverschlüsselt übermittelt wird und nur ein geringer Prozentsatz der Nutzer in der Lage und/oder willens ist, Daten auf dem heimischen Rechner adäquat gegen unbefugte Kenntnisnahme zu sichern, könnte man argumentieren, dass mit den von den Bürgerportalen angebotenen Versand- und Speicherplatzdiensten immerhin ein Sicherheits*fortschritt* erzielt wird – bei gleichzeitiger Wahrung staatlicher Kenntnisnahmemöglichkeiten.

Der so erzielte Fortschritt stellt aber keine Stufe einer weiterführenden Entwicklung zu mehr IT-Sicherheit, sondern eine Sackgasse dar:

- Diejenigen Nutzer, die zu teilnehmerautonomer Verschlüsselung bereit und in der Lage sind, benötigen De-Mail unter dem Sicherheitsaspekt nicht. Sie sind allenfalls an der vereinfachten Behördenkommunikation interessiert.[1685]
- Denjenigen Nutzern, die nicht zu einer teilnehmerautonomen Verschlüsselung bereit oder in der Lage sind, wird suggeriert, dass ihre Daten sicher wären, obwohl sie das de facto *nicht* sind.
- Die *vermeintliche* Sicherheit vermindert dabei aber das Bewusstsein für die Notwendigkeit der Herstellung *echter* Sicherheit. Das Angebot vermeintlicher Sicherheit ist somit nicht Vorstufe zur Schaffung echter Sicherheit, sondern verhindert diese.[1686]

Schließlich ist angesichts der staatlichen Schutzpflichten aus dem Fernmeldegeheimnis (Art. 10 I GG), dem allgemeinen Persönlichkeitsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) und der Eigentums- und Berufsfreiheit (Art. 14 I GG, Art. 12 I GG) äußerst zweifelhaft, ob der Staat in einer verfassungsrechtlichen Perspektive ein System schaffen darf, dass nur einen eingeschränkten Schutz der Vertraulichkeit von Daten bietet – wenn gleichzeitig (und das ist der große Unterschied zur Telekommunikation oder anderer unsicherer Technik) ein umfassenderer Schutz möglich wäre. Spätestens dann, wenn der Staat – wie hier mit der geplanten Ermöglichung der elektronischen Zustellung via Bürgerportal nach § 5a VwZG[1687] – selbst ein solches

1684 Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung vom 16. 04.2009, Datenschutz beim vorgesehenen Bürgerportal unzureichend, verfügbar unter: http://www.sachsen-anhalt.de/LPSA/index.php?type=123&print=1&no_cache=1&id=35083 (09. 12.2009), S. 1.

1685 Interessant wäre insoweit, ob Behörden für eine zusätzliche teilnehmerautonome Verschlüsselung offen wären – was sie in einer verfassungsrechtlichen Perspektive (Schutzpflicht für Fernmeldegeheimnis, Art. 10 I GG, und allgemeines Persönlichkeitsrecht, Art. 2 I GG i.V.m. Art. 1 I GG) sein müssten.

1686 Was im Hinblick auf die staatlichen Kenntnisnahmeoptionen auch durchaus gewollt ist.

1687 Vgl. einzufügenden § 5a Verwaltungszustellungsgesetz [Elektronische Zustellung gegen Zugangsbestätigung über Bürgerportale]: „(1) Die elektronische Zustellung kann im Übrigen unbeschadet des § 5 Absatz 4 und 5 Satz 1 durch Übermittlung nach § 17 des Bürgerportalge-

System zur Kommunikation mit dem Einzelnen nutzen will, muss er *echte* Vertraulichkeit gewährleisten; s.o.:

Dort, wo der Staat selbst unmittelbar die Vertraulichkeit der Fernmeldekommunikation sicherstellen kann, muss er dies auch tun. (s.o. in Teil 6 unter A.I.5.a.dd))

Befinden sich Betriebs- und Geschäftsgeheimnisse hingegen innerhalb der staatlichen Sphäre – und damit außerhalb der Kontrolle und unter Umständen ohne entsprechenden Willen des Geheimnishabers – muss der Staat ihre Vertraulichkeit sicherstellen. (s.o. in Teil 6 unter B.II.2.d.)

Ein Angebot nur vermeintlicher Vertraulichkeit, das die Nutzer in vermeintlicher Sicherheit wiegt und dadurch die Durchsetzung echter Vertraulichkeit hindert, wird daher dem staatlichen Förderungsgebot aus seiner grundrechtlichen Schutzpflicht nicht gerecht.

Zur Lösung des Verschlüsselungsdilemmas kann die Strategie der Verlagerung von Verschlüsselung auf Kommunikationsdiensteanbieter ohnehin weniger beitragen als man auf den ersten Blick vermuten mag: Eine solche Strategie kann allenfalls den Anteil verschlüsselter, staatlichem Mitlesen nicht zugänglicher Daten gering halten und so die technische Möglichkeit der massenhaften Überwachung aufrecht erhalten. All diejenigen, die Daten vor staatlicher Kenntnisnahme bewahren wollen, können und werden dies tun. In diesen Fällen müssen die Sicherheitsbehörden – soweit die gesetzlichen Voraussetzungen vorliegen – mit den Werkzeugen der Online-Durchsuchung und Quellen-TKÜ vorgehen oder andere Erkenntniswege suchen.

Bürgerportale können also – pointiert gesagt – nur die Möglichkeit der staatlichen Kenntnisnahme solcher Daten und Kommunikation sicherstellen, deren Überwachung nicht nötig (keine Straftaten) oder nicht angemessen (keine schwerwiegenden Straftaten) ist. Die Daten, für die staatliche Kenntnisnahmeoptionen bestehen bleiben sollen, finden sich jedenfalls nicht auf Bürgerportalen.

Diese wenig bedeutsamen Kenntnisnahmemöglichkeiten werden erkauft mit der massenhaften Gewährung nur unzureichenden Vertraulichkeitsschutzes. Wo es um Kommunikation mit staatlichen Stellen geht, verstößt die Nutzung von Bürgerportalen, wie sie derzeit umgesetzt werden sollen, gegen grundrechtliche Schutzpflichten (etwa aus dem Fernmeldegeheimnis, Art. 10 I GG, oder aus der Eigentums- und Berufsfreiheit, Art. 14 I GG und Art. 12 I GG). Strategien der Verlagerung von Verschlüsselung auf dritte Diensteanbieter sind daher abzulehnen.

setzes akkreditierter Diensteanbieter gegen Zugangsbestätigung an das Bürgerportalpostfach des Empfängers erfolgen. Bei der Zustellung nach Satz 1 findet § 5 Absatz 4 und 6 mit der Maßgabe Anwendung, dass an die Stelle des Empfangsbekenntnisses die Zugangsbestätigung tritt. […]"; BT-Drs. 16/12598, S. 12.

Auch jüngere Strategien zur Lösung des Verschlüsselungsdilemmas vermochten nicht, den Konflikt der widerstreitenden Freiheits- und Sicherheitsinteressen aufzulösen. Vielleicht scheint es an der Zeit, sich von der Vorstellung, es könne überhaupt eine „Lösung" geben, zu verabschieden.

Kernerkenntnis dieser Arbeit ist jedenfalls, dass es einen wirklich *unantastbaren* grundrechtlichen Kernbestand gibt,[1688] der überwachungsfrei bleiben muss:

> „Zwar wird es stets Formen von besonders gravierender Kriminalität und entsprechende Verdachtssituationen geben, die die Effektivität der Strafrechtspflege als Gemeinwohlinteresse manchem gewichtiger erscheinen lässt als die Wahrung der menschlichen Würde des Beschuldigten. Eine solche Wertung ist dem Staat jedoch durch Art. 1 Abs. 1, Art. 79 Abs. 3 GG verwehrt."[1689]

Dies haben selbst die gewichtigsten Sicherheitsinteressen zu respektieren. Insoweit bleibt kein Spielraum für Abwägungen zwischen Freiheit und Sicherheit. Der durch die Ewigkeitsgarantie gesicherte Kernbestand der Verfassung gibt insoweit eine klare, nicht relativierbare Antwort.

Im alltäglichen, praktischen Umgang mit Verschlüsselung durch die Sicherheitsbehörden folgt daraus die Notwendigkeit eines einzelfallorientierten Ansatzes unter strikter Beachtung des Verhältnismäßigkeitsgrundsatzes:

- Geht es um längerfristige heimliche Beobachtung und Überwachung (Strukturermittlungen) im Bereich mittlerer und schwerer Kriminalität, ist auf andere Ermittlungsmaßnahmen als E-Mail- und Internetüberwachung zurückzugreifen. Denkbar sind der Einsatz verdeckter Ermittler (§ 110a StPO) oder Abhör- (§ 100f StPO) und Observationsmaßnahmen (§ 100h StPO) außerhalb von Wohnungen. Im Übrigen muss auf längerfristige heimliche Überwachung jenseits konkreter Verdachtsmomente verzichtet werden.
- Werden im Zuge von Durchsuchungsmaßnahmen verschlüsselte Daten gefunden, können Dritte bereits nach bestehender Rechtslage gezwungen werden, Passwörter oder Schlüssel herauszugeben, soweit sie solche kennen. Dabei ist vor allem an die Systemadministratoren zu denken: Im gesamten wirtschaftlichen Kontext wird der ganz überwiegende Teil informationstechnischer Systeme von Dritten administriert und nicht vom beschuldigten Mitarbeiter oder Unternehmer selbst. Auch privat administrieren viele ihre informationstechnischen Systeme nicht (vollständig) selbst. Bei vielen verschlüsselten Daten wird sich auf diese Weise eine Kenntnisnahmemöglichkeit bieten. Schließlich ergeben Durchsuchungen regelmäßig vielfältige weitere Erkenntnisquellen.[1690]

1688 Der unantastbare Kernbereich privater Lebensgestaltung wurde dagegen vom BVerfG häufig gerade dann bemüht, wenn im Anschluss die Möglichkeiten der Einschränkung dieses Kernbereichs diskutiert wurden.

1689 BVerfG, Urteil vom 03.03.2004, Az.: 1 BvR 2378/98 und 1 BvR 1084/99, Rn. 121.

1690 Anders allerdings bei Delikten, in denen es nur etwa um den Besitz bestimmter Daten geht, z.B. Kinderpornographie. Kann man diese Daten nicht entschlüsseln, ist die Straftat kaum nachweisbar.

- Verhindert die Verschlüsselung von Daten eine inhaltliche Kenntnisnahme, ist schlicht auf andere Erkenntnisoptionen auszuweichen. Sollte es solche anderen Optionen nicht geben, bleibt nichts anderes als diese Grenze staatlicher Erkenntnis- und Ermittlungsmöglichkeiten hinzunehmen. Kein Staat kann immer alles wissen und alle drohenden Straftaten im Voraus erkennen und verhindern. Und falls doch: Wollten wir in diesem Staat leben?

Literaturverzeichnis

Albrecht, Astrid: Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Baden-Baden 2003.

Albrecht, Hans-Jörg / Dorsch, Claudia / Krüpe, Christian: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen – Abschlussbericht, verfügbar unter: http://www.bmj.bund.de/files/-/134/Abschlussbericht.pdf (26.11.2007).

Alexy, Robert: Theorie der Grundrechte, Baden-Baden 1985.

Andrzejak, Artur: Kryptoregulierung, in: Hoeren, Thomas / Queck, Robert (Hrsg.), Rechtsfragen der Informationsgesellschaft, Berlin 1999, S. 132–145.

Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder: Orientierungshilfe zum Einsatz kryptografischer Verfahren, verfügbar unter: http://www.lda.brandenburg.de/media/2473/kryptoverfahren.pdf (21.04.2008).

Augsberg, Steffen: Denken vom Ausnahmezustand her – Über die Unzulässigkeit der anormalen Konstruktion und Destruktion des Normativen, in: Arndt, Felix / Betz, Nicole / Farahat, Anusch / Goldmann, Matthias (Hrsg.), Freiheit, Sicherheit, Öffentlichkeit – 48. Assistententagung Öffentliches Recht, Baden-Baden 2009, S. 17–39.

Backu, Frieder: Pflicht zur Verschlüsselung?, ITRB 2003, S. 251–253.

Bader, Johann / Ronellenfitsch, Michael (Hrsg.): Beck´scher Online-Kommentar VwVfG, Stand 01.07.2009.

Bär, Wolfgang: Anmerkung zu LG Hamburg, Beschluss vom 01.10.2007, Az.: 629 Qs 29/07, MMR 2008, S. 425–426.

Bär, Wolfgang: Durchsuchungen im EDV-Bereich, CR 1995, S. 158-169, 227-234.

Bär, Wolfgang: Handbuch zur EDV-Beweissicherung, Stuttgart 2007.

Bär, Wolfgang: Wardriver und andere Lauscher – Strafrechtliche Fragen im Zusammenhang mit WLAN, MMR 2005, S. 434–441.

Baum, Michael / Trafkowski, Armin: Verschlüsselung und Strafzumessung, CR 2002, S. 69–73.

Bäumler, Helmut: Das Recht auf Anonymität, in: Bäumler, Helmut / von Mutius, Albert (Hrsg.), Anonymität im Internet – Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Braunschweig 2003, S. 1–11.

Bayerisches Landesamt für Verfassungsschutz / Landesamt für Verfassungsschutz Baden-Württemberg: Wirtschaftsspionage in Baden-Württemberg und Bayern – Daten – Fakten – Hintergründe, verfügbar unter: http://www.sicherheitsforum-bw.de/x_loads/wirtschaftsspionage-20 06.pdf (28. 07.2008).

Benesch, Alexander: Als Notar sicher online im Notarnetz, JurPC 24/2002, verfügbar unter: http://www.jurpc.de/auf satz/20020024.htm (05.02.2009).

Bentham, Jeremy: Panopticon, in: Bentham, Jeremy / Bozovic, Miran (Hrsg.), The Panopticon writings, London u.a. 1995, S. 29–95.

Berg, Wilfried: Der Schutz von Betriebs- und Geschäftsgeheimnissen im öffentlichen Recht unter besonderer Berücksichtigung des Umweltinformationsgesetzes, GewArch 1996, S. 177–183.

Bergemann, Nils: Die Telekommunikationsüberwachung nach der Entscheidung des Bundesverfassungsgerichts zum "großen Lauschangriff", in: Roggan, Fredrik (Hrsg.), Lauschen im Rechtsstaat – Gedächtnisschrift für Hans Lisken, Berlin 2004, S. 69–86.

Beucher, Klaus / Schmoll, Andrea: Kryptotechnologie und Exportbeschränkungen, CR 1999, S. 529–534.

Beukelmann, Stephan: Die Online-Durchsuchung, StraFo 2008, S. 1–8.

Beutelspacher, Albrecht: Ist Kryptographie gut – oder zu gut? – Grundlegende Tatsachen und praktische Konsequenzen, in: Hamm, Rainer / Möller, Klaus Peter (Hrsg.), Datenschutz durch Kryptographie – Ein Sicherheitsrisiko?, Baden-Baden 1998, S. 16–41.

Bizer, Johann: Die Kryptokontroverse – Innere Sicherheit und Sicherungsinfrastrukturen, in: Hammer, Volker (Hrsg.), Sicherungsinfrastrukturen – Gestaltungsvorschläge für Technik, Organisation und Recht, Berlin 1995, S. 179–215.

Bizer, Johann: Forschungsfreiheit und informationelle Selbstbestimmung – Gesetzliche Forschungsregelungen zwischen grundrechtlicher Förderungspflicht und grundrechtlichem Abwehrrecht, Baden-Baden 1992.

Bizer, Johann: Kryptokontroverse – Teilnehmerautonome Verschlüsselung und Innere Sicherheit, in: Kubicek, Herbert (Hrsg.), Multimedia – Technik sucht Anwendung, Heidelberg 1995, S. 214–223.

Bizer, Johann: Nachfrage nach Sicherheit, Privater Vertraulichkeitsschutz und staatliche Sicherheitspolitik in der Telekommunikation, in: Bizer, Johannes / Koch, Hans-Joachim (Hrsg.), Sicherheit, Vielfalt, Solidarität – Ein neues Paradigma des Verfassungsrechts?, Baden-Baden 1998, S. 29–45.

Bizer, Johann: Schutz der Vertraulichkeit in der Telekommunikation, KritJ 1995, S. 450–465.

Bizer, Johann: Verschlüsselung und staatlicher Datenzugriff – Die deutsche Debatte, in: Büllesbach, Alfred (Hrsg.), Datenschutz im Telekommunikationsrecht – Deregulierung und Datensicherheit in Europa, Köln 1997, S. 245–270.

Böckenförde, Ernst-Wolfgang: Grundrechte als Grundsatznormen – Zur gegenwärtigen Lage der Grundrechtsdogmatik, Der Staat 1990, S. 1–31.

Böckenförde, Thomas: Die Ermittlung im Netz – Möglichkeiten und Grenzen neuer Erscheinungsformen strafprozessualer Ermittlungstätigkeit, Tübingen 2003.

Bourquain, Knut: Die Förderung guten Verwaltungshandelns durch Kodizes – Zugleich ein Beitrag zum Europäischen Kodex für gute Verwaltungspraxis, DVBl. 2008, S. 1224–1233.

Bourseau, Frank / Fox, Dirk / Thiel, Christoph: Vorzüge und Grenzen des RSA-Verfahrens, DuD 2002, S. 84–89.

Brands, Gilbert: IT-Sicherheitsmanagement – Protokolle, Netzwerksicherheit, Prozessorganisation, Berlin Heidelberg 2005.

Braun, Torsten: Geschichte und Entwicklung des Internets, InfSpekt 2010, S. 201-207.

Breyer, Patrick: Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, verfügbar unter: http://publikationen.ub.uni-frankfurt.de/volltexte/2005/500/pdf/BreyerPatrick.pdf (21.04.2008).

Brüning, Christoph / Helios, Marcus: Die verfassungsprozessuale Durchsetzung grundrechtlicher Schutzpflichten am Beispiel des Internets, Jura 2001, S. 155–162.

Brunst, Phillip W.: Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen – Zum Spannungsfeld zwischen einem Recht auf Anonymität bei der elektronischen Kommunikation und den Möglichkeiten zur Identifizierung und Strafverfolgung, Berlin 2009.

Bryde, Brun-Otto: Die Effektivität von Recht als Rechtsproblem, Berlin 1993.

Buchmann, Johannes: Einführung in die Kryptographie, 4. Auflage, Berlin 2008.

Buermeyer, Ulf: Die "Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007, S. 154–166, verfügbar unter: http://www.hrr-strafrecht.de/hrr/ar chiv/07-04/index.php?sz=8 (10.08.2009).

Buermeyer, Ulf: Die "Online-Durchsuchung". Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007, S. 329–337, verfügbar unter: http://www .hrr-strafrech t.de/hrr/archiv/07-08/index.php?sz=7 (07.09.2007).

Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2009, verfügbar unter: http://www.bsi.bund.de/literat/lagebericht/Lagebericht2009.pdf (09.03. 2009).

Bundesamt für Sicherheit in der Informationstechnik: IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik, verfügbar unter: http://www.bsi.de/literat/kriterie. htm (13.02.2008).

Bundesministerium des Innern / Bundesministerium der Justiz: Zweiter Periodischer Sicherheitsbericht, verfügbar unter: http://www.bmj.bund.de/files/-/1485/2.%20Periodischer%20Sicherheitsb ericht%20Langfassung.pdf (15.01.2008).

Bundesministerium für Wirtschaft und Arbeit: Handbuch für den Geheimschutz in der Wirtschaft, verfügbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/bmwa-geheimschut zhandbuch,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf (28.06.2007).

Calliess, Christian: Schutzpflichten, § 44, in: Merten, Detlef / Papier, Hans-Jürgen (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Band 2, Grundrechte in Deutschland – Allgemeine Lehren I, Heidelberg 2006.

Chew, Monika / Balfanz, Dirk / Laurie, Ben: (Under)mining Privacy in Social Networks, verfügbar unter: http://w2spconf.com/2008/papers/s 3p2.pdf (12.01.2009).

Cremer, Wolfram: Freiheitsgrundrechte – Funktionen und Strukturen, Tübingen 2003.

Dannecker, Gerhard: Neuere Entwicklungen im Bereich der Computerkriminalität: Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung, BB 1996, S. 1285–1294.

Degen, Thomas A.: Mahnen und Klagen per E-Mail – Rechtlicher Rahmen und digitale Kluft bei Justiz und Anwaltschaft?, NJW 2008, S. 1473–1480.

Denninger, Erhard: Der "große Lauschangriff" auf dem Prüfstand der Verfassung, in: Roggan, Fredrik (Hrsg.), Lauschen im Rechtsstaat – Gedächtnisschrift für Hans Lisken, Berlin 2004, S. 13–24.

Detjen, Markus: Ausstieg ohne Ende? – Die Beendigung der Kernenergienutzung im Spiegel des Verfassungsrechts, Forum Recht Online 2000, verfügbar unter: http://www.forum-recht-online.de/2000/200/200detjen.htm (12.08.2008).

Di Fabio, Udo: Risikoentscheidungen im Rechtsstaat – Zum Wandel der Dogmatik im öffentlichen Recht, insbesondere am Beispiel der Arzneimittelüberwachung, Tübingen 1994.

Diehl, Malte: Kryptographiegesetzgebung im Wandel – Von begrenzten Schlüssellängen zur Schlüsselherausgabe, DuD 2008, S. 243–247.

Diehl, Malte: Sicherheit in der Informationstechnik – der Begriff IT-Sicherheit, InfSpekt 2004, S. 343–353.

Dietlein, Johannes: Die Lehre von den grundrechtlichen Schutzpflichten, Berlin 1992.

Dill, Ricarda: Rundfunkbegriff und Telekommunikationsdienste, in: Haratsch, Andreas / Kugelmann, Dieter / Repkewitz, Ulrich (Hrsg.), Herausforderungen an das Recht der Informationsgesellschaft, Mainz 1996, S. 81–96.

Dix, Alexander: Gesetzliche Verschlüsselungsstandards – Möglichkeiten und Grenzen der Gesetzgebung, CR 1997, S. 38–43.

Dix, Alexander: Neue Perspektiven für den Schutz personenbezogener Daten?, in: Roggan, Fredrik (Hrsg.), Online-Durchsuchungen – Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, Dokumentation einer Fachtagung der Humanistischen Union und der Friedrich-Naumann-Stiftung für die Freiheit am 28. April 2008 in Berlin, Berlin 2008, S. 71–81.

Dolzer, Rudolf / Vogel, Klaus (Begr.): Bonner Kommentar zum Grundgesetz, Heidelberg, Stand Oktober 2009.

Dreier, Horst: Dimensionen der Grundrechte – Von der Wertordnungsjudikatur zu den objektivrechtlichen Grundrechtsgehalten, Hannover 1993.

Dreier, Horst (Hrsg.): Grundgesetz, 2. Auflage, Tübingen 2004.

Düx, Heinz: Globale Sicherheitsgesetze und weltweite Erosion von Grundrechten – Statt „Feindstrafrecht" globaler Ausbau demokratischer Rechte, ZRP 2003, S. 189–195.

Eckert, Claudia: IT-Sicherheit – Konzepte – Verfahren – Protokolle, 5. Auflage, München 2008.

Electronic Privacy Information Center: Cryptography and Liberty 2000 – Executive Summary, verfügbar unter: http://www.stanford.edu/class/msande91si/www-spr04/readings/week6/epic.htm (23.10.2009).

ENISA: Cloud Computing – Benefits, Risks and Rcommendations for Information Security, verfügbar unter: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReportta (23.11.2009).

Epping, Volker / Hillgruber, Christian (Hrsg.): Beck´scher Online-Kommentar Grundgesetz, Stand 01.11.2009.

Ernst, Stefan: Hacker und Computerviren im Strafrecht, NJW 2003, S. 3233–3239.

Faller, Rico: Schächten als Konkurrenzproblem? – Das Urteil des BVerfG aus Sicht der Grundrechtsdogmatik, KritJ 2002, S. 227–233.

Federrath, Hannes: Steganographie – vertrauliche Kommunikation ohne Kryptographie, in: Hamm, Rainer / Möller, Klaus Peter (Hrsg.), Datenschutz durch Kryptographie – Ein Sicherheitsrisiko?, Baden-Baden 1998, S. 42–51.

Federrath, Hannes / Pfitzmann, Andreas: Gliederung und Systematisierung von Schutzzielen in IT-Systemen, DuD 2000, S. 704–710.

Federrath, Hannes / Pfitzmann, Andreas: IT-Sicherheit, in: Wind, Martin / Kröger, Detlef (Hrsg.), Handbuch IT in der Verwaltung, Berlin 2006, S. 273–292.

Fox, Dirk: Stellungnahme zur "Online-Durchsuchung" – Verfassungsbeschwerden 1 BvR 37/03 und 1 BvR 595/07, verfügbar unter: http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf (30.12.2008).

Froomkin, A. Michael: The Metaphor Is The Key: Cryptography, The Clipper Chip, And The Constitution, U. Pa. L. Rev. 1995, S. 709–896.

Galetta, Diana-Urania: Inhalt und Bedeutung des europäischen Rechts auf eine gute Verwaltung, EuR 2007, S. 57–80.

Gassen, Dominik: Digitale Signaturen in der Praxis – Grundlagen, Sicherheitsfragen und normativer Rahmen, Köln 2003.

Gematik GmbH: Die elektronische Gesundheitskarte: whitepaper Sicherheit – Wie werden Gesundheitsdaten in Zukunft geschützt?, verfügbar unter: http://www.gematik.de/(S(vdkzifron3gqkkysw4nr5jro))/Pressemitteilung___09_05_2008.Gematik (26.10.2009).

Geppert, Martin / Piepenbrock, Hermann-Josef / Schütz, Raimund et al. (Hrsg.): Beck'scher TKG-Kommentar, Stand 01.07.2006.

Gercke, Marco: Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit – Der Einsatz softwarebasierter Ermittlungsinstrumente zum heimlichen Zugriff auf Computerdaten, CR 2007, S. 245–253.

Gercke, Marco: Telekommunikationsüberwachung (TKÜ), in: Roggan, Fredrik / Kutscha, Martin (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Auflage, Berlin 2006, S. 146–182.

Gola, Peter / Schomerus, Rudolf (Hrsg.): Bundesdatenschutzgesetz, 9. Auflage, München 2007.

Groß, Thomas: Die Schutzwirkung des Brief-, Post- und Fernmeldegeheimnisses nach der Privatisierung der Post, JZ 1999, S. 326–335.

Groß, Thomas: Terrorbekämpfung und Grundrechte – Zur Operationalisierung des Verhältnismäßigkeitsgrundsatzes, KritJ 2002, S. 1–17.

Grote, Rainer: Kommunikative Selbstbestimmung im Internet und Grundrechtsordnung, KritV 1999, S. 27–56.

Gurlit, Elke: Die Verfassungsrechtsprechung zur Privatheit im gesellschaftlichen und technologischen Wandel, RdV 2006, S. 43–50.

Gusy, Christoph: Rechtsgüterschutz als Staatsaufgabe – Verfassungsfragen der "Staatsaufgabe Sicherheit", DÖV 1996, S. 573–583.

Hadamek, Ruth: Art. 10 GG und die Privatisierung der Deutschen Bundespost, Berlin 2002.

Hamm, Rainer: Kryptokontroverse, DuD 1997, S. 186–191.

Hammer, Volker: Die 2. Dimension der IT-Sicherheit – Verletzlichkeitsreduzierende Technikgestaltung am Beispiel von Public Key Infrastrukturen, Braunschweig 1999.

Hammer, Volker: Gestaltungsbedarf und Gestaltungsoptionen für Sicherungsinfrastrukturen, in: Hammer, Volker (Hrsg.), Sicherungsinfrastrukturen – Gestaltungsvorschläge für Technik, Organisation und Recht, Berlin 1995, S. 41–86.

Hannich, Rolf (Hrsg.): Karlsruher Kommentar zur Strafprozessordnung, 6. Auflage, 2008.

Hansen, Markus / Pfitzmann, Andreas: Techniken der Online-Durchsuchung: Gebrauch, Missbrauch, Empfehlungen, in: Roggan, Fredrik (Hrsg.), Online-Durchsuchungen – Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, Dokumentation einer Fachtagung der Humanistischen Union und der Friedrich-Naumann-Stiftung für die Freiheit am 28. April 2008 in Berlin, Berlin 2008, S. 131–154.

Hansen, Markus / Pfitzmann, Andreas: Windei Bundestrojaner – Online-Durchsuchung vs. Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme, verfügbar unter: http://www.heise.de/ct/artikel/Windei-Bundestrojaner-291808.html (10.11.2009).

Hansen, Markus / Pfitzmann, Andreas / Roßnagel, Alexander: Online-Durchsuchung, DRiZ 2007, S. 225–230.

Härting, Niko: Unverschlüsselte E-Mails im anwaltlichen Geschäftsverkehr – Ein Verstoß gegen die Verschwiegenheitspflicht?, MDR 2001, S. 61–63.

Hartmann, Jörg: Sichere Kommunikation im Internet, verfügbar unter: http://deposit.ddb.de/cgi-bin/dokserv?idn=967128323&dok_var=d1&dok_ext=pdf&filename=967128323.pdf (21.04.2008).

Heckmann, Dirk: Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen – Maßstäbe für ein IT-Sicherheitsrecht, MMR 2006, S. 280–285.

Hefermehl, Wolfgang / Köhler, Helmut / Bornkamm, Joachim (Hrsg.): Gesetz gegen den unlauteren Wettbewerb, 26. Auflage, München 2008.

Heidrich, Jörg: Rechtliche Fragen bei der Verwendung von DNS-Blacklisting zur Spam-Filterung, CR 2009, S. 168–173.

Hemmer, Philip / Wrachtrup, Jörg: Where Is My Quantum Computer?, Science 2009, S. 473–474, verfügbar unter: http://www.sciencemag.org/cgi/reprint/324/5926/473.pdf (08.06.2009).

Hermann, Dieter: Werte und Kriminalität – Konzeption einer allgemeinen Kriminalitätstheorie, Wiesbaden 2003.

Hermes, Georg: Das Grundrecht auf Schutz von Leben und Gesundheit – Schutzpflicht und Schutzanspruch aus Art. 2 Abs. 2 Satz 1 GG, Heidelberg 1987.

Hermes, Georg: Staatliche Infrastrukturverantwortung – Rechtliche Grundstrukturen netzgebundener Transport- und Übertragungssysteme zwischen Daseinsvorsorge und Wettbewerbsregulierung am Beispiel der leitungsgebundenen Energieversorgung in Europa, Tübingen 1998.

Heß, Reinhold: Grundrechtskonkurrenzen – Zugleich ein Beitrag zur Normstruktur der Freiheitsrechte, Berlin 2000.

Heuser, Ansgar: Verschlüsselung im Spannungsfeld von staatlichem Anspruch und individueller Freiheit – ein Beitrag zur 'Kryptokontroverse', in: Kubicek, Herbert (Hrsg.), Multimedia – Technik sucht Anwendung, Heidelberg 1995, S. 224–228.

Hirsch, Burkhard: Bemerkungen zu den Entwürfen eines Gesetzes zur Umsetzung des Urteils des Bundesverfassungsgerichts v. 03. März 2004, in: Roggan, Fredrik (Hrsg.), Lauschen im Rechtsstaat – Gedächtnisschrift für Hans Lisken, Berlin 2004, S. 87–98.

Hoeren, Thomas: Skript Internetrecht (Stand Sept. 2009), verfügbar unter: http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_September2009.pdf (05.06.2009).

Hoeren, Thomas: Skript Internetrecht (Stand Feb. 2010), verfügbar unter: http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Internetrecht_Februar2010.pdf (30.03.2010).

Hoffmann-Riem, Wolfgang: Informationelle Selbstbestimmung in der Informationsgesellschaft – Auf dem Weg zu einem neuen Konzept des Datenschutzes, AöR 1998, S. 513–540.

Hofmann, Manfred: Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmaßnahme?, NStZ 2005, S. 121–125.

Höhne, Focke / Dienst, Sebastian: Das Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen (Zugangserschwerungsgesetz – ZugErschwG), juris PR ITR 13/2009, Anm. 6.

Holtschneider, Rainer: Normenflut und Rechtsversagen – Wie wirksam sind rechtliche Regelungen?, Baden-Baden 1991.

Holznagel, Bernd: Recht der IT-Sicherheit, München 2003.

Hornung, Gerrit: Ein neues Grundrecht, CR 2008, S. 299–306.

Hornung, Gerrit: Ermächtigungsgrundlage für die "Online-Durchsuchung"? – Verfassungsrechtliche Anforderungen an und Grenzen für den heimlichen Zugriff auf IT-Systeme im Ermittlungsverfahren, DuD 2007, S. 575–580.

Huber, Ernst Rudolf: Der Streit um das Wirtschaftsverfassungsrecht (Teil 2), DÖV 1956, S. 135–143.

Hufen, Friedhelm: Schutz der Persönlichkeit und Recht auf informationelle Selbstbestimmung, in: Badura, Peter / Dreier, Horst (Hrsg.), Festschrift 50 Jahre Bundesverfassungsgericht, Band 2, Tübingen 2001, S. 105–125.

Huhn, Michaela / Pfitzmann, Andreas: Plädoyer gegen verbindliche staatliche Kryptoregulierung, DSB 1996, S. 2–5.

Huhn, Michaela / Pfitzmann, Andreas: Technische Randbedingungen jeder Kryptoregulierung, verfügbar unter: http://events.ccc.de/congress/1995/div/pfitz/krypto.htm (18.12.2006).

Hullen, Nils: Grundlagen und aktuelle Fragen des Medienrechts – Tagungsbericht der Cottbuser Medienrechtstage, JurPC 128/2008, verfügbar unter: http://www.jurpc.de/aufsatz/20080128.htm (09.06.2009).

Ihde, Rainer: Cookies – Datenschutz als Rahmenbedingung der Internetökonomie, CR 2000, S. 413–423.

Ipsen, Knut (Hrsg.): Völkerrecht, 5. Auflage, München 2004.

Isensee, Josef: Anwendung der Grundrechte auf juristische Personen, § 118, in: Isensee, Josef / Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band V, Allgemeine Grundrechtslehren, 2. Auflage, Heidelberg 2000.

Isensee, Josef: Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, § 111, in: Isensee, Josef / Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band V, Allgemeine Grundrechtslehren, 2. Auflage, Heidelberg 2000.

Isensee, Josef: Das Grundrecht auf Sicherheit, Berlin u.a. 1983.

Jakobs, Michael Ch.: Der Grundsatz der Verhältnismäßigkeit – Mit einer exemplarischen Darstellung seiner Geltung im Atomrecht, Köln 1985.

Jarass, Hans D.: Grundrechte als Wertentscheidungen bzw. objektivrechtliche Prinzipien in der Rechtsprechung des Bundesverfassungsgerichts, AöR 1985, S. 363–397.

Jarass, Hans D. / Pieroth, Bodo (Hrsg.): Grundgesetz für die Bundesrepublik Deutschland – Kommentar, 10. Auflage, München 2009.

Joecks, Wolfgang / Miebach, Klaus (Hrsg.): Münchener Kommentar zum Strafgesetzbuch, München 2003.

Kahl, Wolfgang: Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz – Zugleich ein Beitrag zur Lehre der Grundrechtskonkurrenzen, Tübingen 2000.

Kintzi, Heinrich: Externe Datenverarbeitung von Berufsgeheimnissen im Kontext von § 203 StGB – Verletzung von Privatgeheimnissen, Gutachten der Großen Strafrechtskommission des Deutschen Richterbundes, DRiZ 2007, S. 244–249.

Klett, Detlef / Lee, Sang-Woon: Vertraulichkeit des E-Mailverkehrs, CR 2008, S. 644–648.

Kloepfer, Michael (Hrsg.): Informationsrecht, München 2002.

Knopp, Michael / Wilke, Daniel / Hornung, Gerrit, et al.: Grunddienste für die Rechtssicherheit elektronischer Kommunikation – Rechtlicher Bedarf für eine gewährleistete Sicherheit, MMR 2008, S. 723–728.

Koch, Alexander: Grundrecht auf Verschlüsselung?, CR 1997, S. 106–110.

Koch, Hans-Joachim / Roßnagel, Alexander: Neue Energiepolitik und Ausstieg aus der Kernenergie, NVwZ 2000, S. 1–9.

Koch, Robert: Haftung für die Weiterverbreitung von Viren durch E-Mails, NJW 2004, S. 801–807.

Köhntopp, Marit / Köhntopp, Kristian: Datenspuren im Internet, verfügbar unter: http://kris.koehntopp.de/artikel/datenspuren/CR_Datenspuren_im_Internet.pdf (05.05.2009).

Koops, Bert-Jaap: Crypto Law Survey (Stand 01.07.2008), verfügbar unter: http://rechten.uvt.nl/koops/cryptolaw/cls2.htm (23.10.2009).

Koops, Bert-Jaap: The crypto controversy – A key conflict in the Information Society, Den Haag 1999.

Kraft, Dennis / Meister, Johannes: Die Strafbarkeit von Internet-Demonstrationen – Zugleich eine Besprechung des "Online-Demo"-Urteils des AG Frankfurt a.M. vom 01.07.2005 - 991 Ds 6199 Js 226314/01, K&R 2005, S. 458–462.

Kraft, Dennis / Meister, Johannes: Rechtsprobleme virtueller Sit-ins, MMR 2003, S. 366–374.

Kuner, Christopher: Rechtliche Aspekte der Datenverschlüsselung im Internet, NJW-CoR 1995, S. 413–418.

Kuner, Christopher: Rechtsprobleme der Kryptografie (Stand August 2006), in: Hoeren, Thomas / Sieber, Ulrich (Hrsg.), Recht – Technik – Wirtschaft, Handbuch Multimedia-Recht – Rechtsfragen des elektronischen Geschäftsverkehrs, München, Teil 17.

Künnemann, Robert: Funknetzwerke und ihre Sicherheit, JurPC 62/2009, verfügbar unter: http://www.jurpc.de/aufsatz/20090062.htm (25.03.2009).

Kutscha, Martin: Innere Sicherheit – Föderale Kompetenzverteilung, Unitarisierung und Internationalisierung, in: Roggan, Fredrik / Kutscha, Martin (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Auflage, Berlin 2006, S. 78–104.

Kutscha, Martin: Innere Sicherheit und Freiheitsrechte, in: Roggan, Fredrik / Kutscha, Martin (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Auflage, Berlin 2006, S. 28–61.

Kutscha, Martin / Roggan, Fredrik: Große Lauschangriffe im Polizeirecht – Konsequenzen des Karlsruher Richterspruchs, in: Roggan, Fredrik (Hrsg.), Lauschen im Rechtsstaat – Gedächtnisschrift für Hans Lisken, Berlin 2004, S. 25–45.

Lackner, Karl / Kühl, Kristian (Hrsg.): Strafgesetzbuch – Kommentar, 26. Auflage, München 2007.

Langheinrich, Marc: Gibt es in einer total informatisierten Welt noch eine Privatsphäre?, in: Mattern, Friedemann (Hrsg.), Die Informatisierung des Alltags – Leben in smarten Umgebungen, Berlin Heidelberg 2007, verfügbar unter: http://dx.doi.org/10.1007/978-3-540-71455-2 (29.03. 2008), S. 233–264.

Laprie, Jean-Claude: Dependability of Computer Systems: from Concepts to Limits, IFIP International Workshop on Dependable Computing and its Applications (DCIA´98), Johannesburg, 12.-14. Januar 1998, S. 108–126.

Lepsius, Oliver: Das Computer-Grundrecht: Herleitung – Funktion – Überzeugungskraft, in: Roggan, Fredrik (Hrsg.), Online-Durchsuchungen – Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, Dokumentation einer Fachtagung der Humanistischen Union und der Friedrich-Naumann-Stiftung für die Freiheit am 28. April 2008 in Berlin, Berlin 2008, S. 21–56.

Lepsius, Oliver: Das Verhältnis von Sicherheit und Freiheitsrechten in der Bundesrepublik Deutschland nach dem 11. September 2001, verfügbar unter: http://www.aicgs.org/documents/lepsius.pdf (04.12.2009).

Libertus, Michael: Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren, MMR 2005, S. 507–512.

Lindloff, Dirk: E-Mail-Kommunikation von Rechtsanwälten mit Mandanten und Gerichten, Marburg 2005.

Lübbe-Wolff, Gertrude: Die Grundrechte als Eingriffsabwehrrechte – Struktur und Reichweite der Eingriffsdogmatik im Bereich staatlicher Leistungen, Baden-Baden 1988.

Luch, Anika D. / Schulz, Sönke E.: eDaseinsvorsorge – Neuorientierung des überkommenen (Rechts-)Begriffs "Daseinsvorsorge" im Zuge technischer Entwicklungen?, MMR 2009, S. 19–24.

Marauhn, Thilo: Sicherheit in der Kommunikationstechnik durch legislatives Risikomanagement, KritV 1999, S. 57–90.

Marly, Jochen (Hrsg.): Praxishandbuch Softwarerecht – Rechtsschutz und Vertragsgestaltung, 5. Auflage, München 2009.

Mattern, Friedemann: Pervasive/Ubiquitous Computing, InfSpekt 2001, S. 145–147.

Maunz, Theodor / Dürig, Günter (Hrsg.): Grundgesetz – Kommentar, Stand Mai 2009, München 1958.

Meier, Bernd-Dieter: Strafrechtliche Sanktionen, Berlin Heidelberg 2006.

Menezes, Alfred J. / van Oorschot, Paul C. / Vanstone, Scott A.: Handbook of applied cryptography, Boca Raton 2001.

Mes, Peter (Hrsg.): Patentgesetz, Gebrauchsmustergesetz – Kommentar, 2. Auflage, München 2005.

Meyer, Jürgen (Hrsg.): Charta der Grundrechte der Europäischen Union, 2. Auflage, Baden-Baden 2006.

Meyerdierks, Per: Sind IP-Adressen personenbezogene Daten?, MMR 2009, S. 8–13.

Meyer-Goßner, Lutz (Hrsg.): Strafprozessordnung, 51. Auflage, München 2008.

Meyer-Wieck, Hannes: Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung („großer Lauschangriff“) nach § 100c Abs. 1 Nr. 3 StPO – Eine rechtstatsächliche Untersuchung im Auftrag des Bundesministeriums der Justiz, verfügbar unter: http://www. bmj.bund.de/files/-/786/Gutachten Wohnraum%FCberwachung.pdf (26.11.2007).

Meyn, Christian: Verschlüsselung und Innere Sicherheit – Die verfassungsrechtliche Zulässigkeit eines Verschlüsselungsverbots bei elektronischer Datenkommunikation, Wiesbaden 2003.

Möller, Hauke: Regulierung anonymer E-Mail – Verfassungsrechtliche Vorgaben, DuD 2000, S. 267–274.

Möstl, Markus: Die staatliche Garantie für die öffentliche Sicherheit und Ordnung – Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union, Tübingen 2002.

Möstl, Markus: Probleme der verfassungsprozessualen Geltendmachung gesetzgeberischer Schutzpflichten – Die Verfassungsbeschwerde gegen legislatives Unterlassen, DÖV 1998, S. 1029–1039.

Muñoz Bellvehí, Xavier / Herreros Margarit, Ignacio / Nolla Puertas, Josep Maria: Derecho de las Telecomunicaciones, 2. Auflage, 2006.

Nitz, Gerhard: Private und öffentliche Sicherheit, Berlin 2000.

Ossenbühl, Fritz: Staatshaftungsrecht, 5. Auflage, München 1998.

Palandt, Otto (Hrsg.): Bürgerliches Gesetzbuch, 68. Auflage, München 2009.

Paul, Reiner: Rechtliche Gemengelagen kommunaler Internetauftritte in Rheinland-Pfalz unter Berücksichtigung von E-Government, JurPC 144/2008, verfügbar unter: http://www.jurpc.de/aufsatz/20080144.htm (17.09.2008).

Pfitzmann, Andreas: Contra Online-Durchsuchung, InfSpekt 2008, S. 65–69.

Pfitzmann, Andreas: Möglichkeiten und Grenzen von Anonymität, in: Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (Hrsg.), Datenschutz und Anonymität, S. 9–20.

Pfitzmann, Andreas / Steinbrecher, Sandra: Digitale Glaubwürdigkeit und Privatsphäre in einer vernetzten Gesellschaft, in: Klumpp, Dieter / Kubicek, Herbert / Roßnagel, Alexander (Hrsg.), Next generation information society? – Notwendigkeit einer Neuorientierung, Mössingen-Talheim 2003, S. 290–299.

Piper, Henning / Ohly, Ansgar (Hrsg.): Gesetz gegen den unlauteren Wettbewerb – Kommentar, 4. Auflage, München 2006.

Pohl, Hartmut: Zur Technik der heimlichen Online-Durchsuchung, DuD 2007, S. 684–688.

Pohlmann, Norbert / Hesse, Malte: Kryptographie: Von der Geheimwissenschaft zur alltäglichen Nutzanwendung (II) – Elementare Verschlüsselungsverfahren, ITSD 2006, S. 430–439, verfügbar unter: http://www.internet-sicherheit.de/fileadmin/docs/publikationen/ITSD-Sicherheit-Artikel-Pohlmann-06-07.pdf (21.4.2008).

Preuß, Ulrich K.: Risikovorsorge als Staatsaufgabe – Die epistemologischen Voraussetzungen von Sicherheit, in: Grimm, Dieter (Hrsg.), Staatsaufgaben, Baden-Baden 1994, S. 523–551.

Radtke, Henning: Aktive Mitwirkungspflichten und die "freiwillige" aktive Mitwirkung des Betroffenen bei dem Zugriff auf elektronisch gespeicherte Daten im Strafprozess – Überlegungen am Beispiel der sog. Bankendurchsuchungen, in: Eser, Albin / Goydke, Jürgen / Maatz, Kurt Rüdiger / Meurer, Dieter (Hrsg.), Strafverfahrensrecht in Theorie und Praxis – Festschrift für Lutz Meyer-Gossner zum 65. Geburtstag, München 2001, S. 321–346.

Raepple, Martin: Sicherheitskonzepte für das Internet – Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, Heidelberg 2001.

Rihaczek, Karl: Kryptokontroverse und Normung, in: Tinnefeld, Marie-Theres / Köhler, Klaus / Piazolo, Michael (Hrsg.), Arbeit in der mobilen Kommunikationsgesellschaft – Arbeits-, datenschutzrechtliche, wirtschaftliche und soziale Auswirkungen der Telearbeit, Braunschweig 1996, S. 270–274.

Robbers, Gerhard: Sicherheit als Menschenrecht – Aspekte der Geschichte, Begründung und Wirkung einer Grundrechtsfunktion, Baden-Baden 1987.

Rohlf, Dietwalt: Der grundrechtliche Schutz der Privatsphäre – Zugleich ein Beitrag zur Dogmatik des Art. 2 Abs. 1 GG, Berlin 1980.

Ronellenfitsch, Michael: Datennotwehr, DuD 2008, S. 110–116.

Rössler, Beate: Der Wert des Privaten, verfügbar unter: http://www.aec.at/de/festival2007/topics/d_roessler_lang.pdf (06.09.2007).

Roßnagel, Alexander: Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger – Thesen zur Änderung der Staatsaufgaben in einer "civil information society", ZRP 1997, S. 26–30.

Roßnagel, Alexander: Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003.

Roßnagel, Alexander: Informationelle Selbstbestimmung in der Welt des Ubiquitous Computing, in: Mattern, Friedemann (Hrsg.), Die Informatisierung des Alltags – Leben in smarten Umgebungen, Berlin Heidelberg 2007, S. 265–289.

Roßnagel, Alexander / Pfitzmann, Andreas: Datenschutz im Internet – Welche Standards informationeller Selbstbestimmung braucht das Internet?, in: Staudt, Erwin (Hrsg.), Deutschland online – Standortwettbewerb im Informationszeitalter; Projekte und Strategien für den Sprung an die Spitze, Berlin 2002, S. 89–98.

Roßnagel, Alexander / Pfitzmann, Andreas / Garstka, Hansjürgen: Modernisierung des Datenschutzrechts, verfügbar unter: http://www.computerundrecht.de/media/gutachten.pdf (02.12. 2008).

Roßnagel, Alexander / Schnabel, Christoph: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, S. 3534–3538.

Rüttgers, Jürgen: Telekommunikation und Datenvernetzung – eine Herausforderung für Gesellschaft und Recht, CR 1996, S. 51–56.

Rux, Johannes: Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden – Rechtsfragen der "Online-Durchsuchung", JZ 2007, S. 285–295.

Sachs, Michael: Grundgesetz – Kommentar, 5. Auflage, München 2009.

Sankol, Barry: Überwachung von Internet-Telefonie, CR 2008, S. 13–18.

Schaar, Peter / Landwehr, Sebastian: Anmerkung zu BGH, Beschl. v. 31.01.2007 – StB 18/06, K&R 2007, S. 202–205.

Scherf, Uwe J. / Schmieszek, Hans-Peter / Viefhues, Wolfram: Elektronischer Rechtsverkehr, Heidelberg 2006.

Scheule, Rupert M.: Das "Digitale Gefälle" als Gerechtigkeitsproblem, InfSpekt 2005, S. 474–488.

Schlegel, Stephan: "Beschlagnahme" von E-Mail-Verkehr beim Provider, HRRS 2007, S. 44–51, verfügbar unter: http://www.hrr-strafrecht.de/hrr/archiv/07-02/index.php?sz=6 (10.08.2009).

Schlink, Bernhard: Abwägung im Verfassungsrecht, Berlin 1976.

Schmeh, Klaus: Kryptografie und Public-Key-Infrastrukturen im Internet, Heidelberg 2001.

Schmitt Glaeser, Walter: Schutz der Privatsphäre, § 129, in: Isensee, Josef / Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band VI, Freiheitsrechte, 2. Auflage, Heidelberg 2001.

Schneier, Bruce: Angewandte Kryptographie – Protokolle, Algorithmen und Sourcecode in C, München 2002.

Schneier, Bruce: Secrets and Lies – Digital security in a networked world, Indianapolis 2004.

Schoch, Friedrich: Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, in: Vereinigung der Deutschen Staatsrechtslehrer (Hrsg.), Der Grundrechtseingriff – Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Osnabrück vom 1. bis 4. Oktober 1997, Band 57, Berlin 1998, S. 158–215.

Schoch, Friedrich: Das Grundrecht der freien Entfaltung der Persönlichkeit in der Rechtsprechung des Bundesverfassungsgerichts, AöR 1975, S. 80-130, 265-290.

Scholz, Rupert / Pitschas, Rainer: Informationelle Selbstbestimmung und staatliche Informationsverantwortung, Berlin 1984.

Schönke, Adolf / Schröder, Horst (Hrsg.): Strafgesetzbuch, 27. Auflage, 2006.

Schwenk, Jörg: Sicherheit und Kryptographie im Internet – Von sicherer E-Mail bis zu IP-Verschlüsselung, 2. Auflage, Wiesbaden 2005.

Seidel, Gerd: Das Versammlungsrecht auf dem Prüfstand, DÖV 2002, S. 283–291.

Sick, Philipp: Objektiv-rechtlicher Gewährleistungsgehalt oder Abwehrfunktion des neuen "Computergrundrechts"? – Anmerkung zum Urteil des BVerfG vom 27.02.2008 (NJW 2008, 822 ff.) zum NRWVerfSchG, VBlBW 2009, S. 85–91.

Sieber, Ulrich / Nolde, Malaika: Sperrverfügungen im Internet – Nationale Rechtsdurchsetzung im globalen Cyberspace?, Berlin 2008.

Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz, 6. Auflage, Baden-Baden 2006.

Soergel, Hans Theodor (Hrsg.): Bürgerliches Gesetzbuch, Band 2a, 13. Auflage, Stuttgart 2002.

Sonntag, Matthias: IT-Sicherheit kritischer Infrastrukturen – Von der Staatsaufgabe zur rechtlichen Ausgestaltung, München 2005.

Speichert, Horst: Praxis des IT-Rechts – Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung, Wiesbaden 2007.

Spies, Axel: USA: Personalisierte Werbung und gläserne Websurfer – Deep Packet Inspection, MMR 2008, S. XII–XIV.

Spindler, Gerald: Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären – Studie im Auftrag des BSI, verfügbar unter: https://www.bsi.bund.de/cae/servlet/contentblob/486890/publicationFile/30666/Gutachten_pdf.pdf;jsessionid=A2EBB4098A4A5164D2E86814BBC18AEC (04.09.2009).

Spranger, Tade Matthias: Die Figur der "Schutzbereichsverstärkung", NJW 2002, S. 2074–2076.

Statewatch: The Shape of Things to Come – EU Future report, verfügbar unter: http://www.statewatch.org/analyses/the-shape-of-things-to-come.pdf (11.09.2008).

Stoll, Peter-Tobias: Sicherheit als Aufgabe von Staat und Gesellschaft – Verfassungsordnung, Umwelt- und Technikrecht im Umgang mit Unsicherheit und Risiko, Tübingen 2003.

Störing, Marc: Strafprozessuale Zugriffsmöglichkeiten auf E-Mail-Kommunikation, Berlin 2007.

Streng, Franz: Strafrechtliche Sanktionen – Die Strafzumessung und ihre Grundlagen, 2. Auflage, Stuttgart 2002.

Stüer, Bernhard / Loges, Sandra: Ausstieg aus der Atomenergie zum Nulltarif?, NVwZ 2000, S. 9–15.

TAUCIS: Technikfolgenabschätzungsstudie Ubiquitäres Computing, verfügbar unter: http://www.taucis.hu-berlin.de/_download/TAUCIS_Studie.pdf (25.09.2008).

Trute, Hans-Heinrich: Der Schutz personenbezogener Informationen in der Informationsgesellschaft, JZ 1998, S. 822–831.

Trute, Hans-Heinrich: Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, in: Vereinigung der Deutschen Staatsrechtslehrer (Hrsg.), Der Grundrechtseingriff – Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Osnabrück vom 1. bis 4. Oktober 1997, Berlin 1998, S. 216–268.

Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein: Verkettung digitaler Identitäten – Untersuchung im Auftrag des Bundesministeriums für Bildung und Forschung, verfügbar unter: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf (05.11.2007).

Unruh, Peter: Zur Dogmatik der grundrechtlichen Schutzpflichten, Berlin 1996.

Valerius, Brian: Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet – Hoheitliche Recherchen in einem grenzüberschreitenden Medium, Berlin 2004.

Volkmann, Uwe: Anmerkung zu BVerfG, Urteil vom 15.01.2002, Az.: 1 BvR 1783/99, DVBl. 2002, S. 332–336.

von Bonin, Andreas: Die Kontrolle digitaler Kommunikationsinhalte – Grenzen staatlicher Regelung und Möglichkeiten kooperativer Kontrolle, Baden-Baden 2000, verfügbar unter: http://www.a-von-bonin.de/Diss/Dissmaster.html (23.09.2008).

von Heintschel-Heinegg, Bernd (Hrsg.): Beck´scher Online-Kommentar StGB, Stand 01.10.2009.

von Mangoldt, Hermann / Klein, Friedrich / Starck, Christian (Hrsg.): Kommentar zum Grundgesetz, 5. Auflage, München 2005.

von Münch, Ingo / Kunig, Philip (Hrsg.): Grundgesetz – Kommentar, 5. Auflage, München 2000.

von Mutius, Albert: Anonymität als Element des allgemeinen Persönlichkeitsrechts – terminologische, rechtssystematische und normstrukturelle Grundfragen, in: Bäumler, Helmut / von Mutius, Albert (Hrsg.), Anonymität im Internet – Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Braunschweig 2003, S. 12–26.

Wagner, Christoph / Lerch, Janusz-Alexander: Mandatsgeheimnis im Internet? – Zur Zulässigkeit anwaltlicher E-Mail-Korrespondenz im Hinblick auf straf- und standesrechtliche Vorgaben, NJW-CoR 1996, S. 380–385.

Wahl, Rainer / Appel, Ivo: Prävention und Vorsorge: Von der Staatsaufgabe zur rechtlichen Ausgestaltung, in: Wahl, Rainer (Hrsg.), Prävention und Vorsorge – Von der Staatsaufgabe zu den verwaltungsrechtlichen Instrumenten, Bonn 1995, S. 1–216.

Wahl, Rainer / Masing, Johannes: Schutz durch Eingriff, JZ 1990, S. 553–563.

Wandtke, Artur-Axel / Bullinger, Winfried (Hrsg.): Praxiskommentar zum Urheberrecht, 2. Auflage, München 2006.

Weichert, Thilo: Bürgerrechtskonforme Bekämpfung der Computerkriminalität, DuD 2007, S. 590–594.

Wittreck, Fabian: Religionsfreiheit als Rationalisierungsverbot – Anmerkungen aus Anlaß der Schächtentscheidung des Bundesverfassungsgerichts, Der Staat 2003, S. 519–555.

Zöller, Mark Alexander: Allgemeine Grundsätze bei Datenübermittlungen von Sicherheitsbehörden, in: Roggan, Fredrik / Kutscha, Martin (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Auflage, Berlin 2006, S. 448–470.